A Schools Guide to **Filter Avoidance**

This guide explores how & why students are looking to bypass school network filtering and offers guidance on how to identify when it's happening and how to respond.

Linewize by Qoria

Introduction

Having a filtered network at school not only serves as a form of safety for students online, but also helps to ensure the internet remains a **powerful tool for learning, rather than a gateway to distraction.**

For young students, the lure of social media, gaming, and other forms of online entertainment is strong and can lead to efforts by students to bypass these filters to gain access to distracting or unsafe content.

VPN

In **excess of 50% senior students** are using or attempting to use a VPN.

Linewize data collected 2022

Hotspotting

30% of students from years 7-11 are suspected of hotspotting at school.

Linewize data collected 2022

School Networks

The top reasons students are using VPN's is to **overide school networks.**

Linewize data collected 2022

What is Filter Avoidance?

Put simply, filter avoidance refers to the student efforts to **circumvent filtering technology** placed on the school network to access inappropriate, unsafe, or distracting online content.

While tactics employed involve technology, the issue is recognised as behavioural rather than technological. There are several methods students can employ; according to Linewize data, the two main tactics are the use of VPNs and hotspotting.

Mobile Data & Hotspotting

Ownership of 4G (and now 5G) enabled smartphones are almost universal in K-12 schools. And with unlimited data plans much more affordable, students are often equipped with as much data as they want to access online content.

Hotspotting is a way of sharing the mobile network and data with other devices - that could be with other phones, tablets, or laptops. Hotspotting has become more accessible with one student hotspot able to have up to 10 other student devices connected. Even when a phone is away in a bag, or in a locker, it can still have the hotspot switched on and used by students.

VPNs

A VPN, or Virtual Private Network, allows a user to connect their computer to a private network, creating an encrypted connection that masks their IP address. It is essentially a way of 'hiding' online. There are legitimate uses for VPNs, mostly relating to privacy and security. However, VPNs can also be used to 'trick' a school network and bypass its filter settings.

There are numerous free and paid VPN services, with new services cropping up every day. Data collected by Linewize suggests that up to half of middle and high students have either installed or tried to use a free web-based VPN at school.

Why do Students Try to Avoid Filters?

Today's children are being introduced to the internet at an increasingly early age and almost exclusively their foundation experiences online are for entertainment purposes. As students continue to spend more time online in the classroom and for education, the temptation to use the internet at school the same way as at home is becoming increasingly hard to resist.

Most schools have some kind of filtering system in place; to access blocked content students turn to filter avoidance tactics. These efforts open the doors to distraction & risk and can negatively impact learning opportunities.

The Problem for Schools and Students

Distraction that undermines learning

In addition to blocking access to unsafe or inappropriate content, school filtering removes the many distractions that can undermine device-based learning activities. Social media, YouTube, online gaming, streaming services etc. are just a few examples of the types of content being accessed by students and diverting attention away from learning. Let's not forget that developmentally, the ability to self-regulate behaviour is still developing well into the Twenties, meaning that staying on task is something that students need a little help with.

Provides a gateway to unsafe content

Schools need to provide students with a safe learning environment that extends to the online world. Students that bypass filters to access content that is risky, inappropriate, or otherwise unsafe, put the wellbeing of themselves and those around them at risk.

Increases teacher workload

Consistent with their duty of care to students, teachers are required to adequately supervise students when using digital technology in the classroom. A teacher's ability to effectively fulfil this duty and simultaneously focus on teaching can be significantly disrupted by students bypassing school filters to access content or activities that are unsuitable or unsafe.

How Schools Can Respond

Set clear expectations

Ensure that your school policies clearly describe what is and isn't permitted when accessing the internet at school. Some key things to consider include:

- **What is the expectation** of students bringing personal devices with mobile data onto school premises?
- Does your school IT policy **explicitly address students hotspotting?**
- **What are the rules** around using VPNs?
- What **steps can teachers take** if they find students breaking these rules? For example, can teachers confiscate student devices? If so, this needs to be stipulated in school Acceptable Use Agreements and signed by parents and students.

Collaborate with students and parents in the policy development to ensure buy-in and comprehension of what the school is striving to achieve.

Monitor and evaluate effectiveness

In cases such as these, the knowledge of one student breaking the rules can be an indicator of more students participating in the behaviour without getting caught. If staff are reporting students bypassing the school filters, take this as an indication that something in the current approach is not working as planned.

Seek to understand why students are bypassing school filters. Are they trying to access games during class time? If so, is this because they are disengaged or, perhaps struggling with the topic being taught? In some cases, bypassing school filters may be an indicator of an underlying student issue that needs to be addressed.

> "It's a bit of a cat and mouse game just trying to keep one step ahead of the technology, and particularly around things like the usage of VPNs. But I know that when a new VPN has been created, **Linewize is ahead of the game** and has blocked that new one."
>
> **Veronica Stevens**
> Deputy Principal, Wellesley College

How Schools Can Respond cont.

Get students and parents onside

Students attempting to do the wrong thing, and a lack of support from parents on issues related to personal devices, can stem from a lack of understanding around why the school has chosen a given approach or set of rules. To get both students and parents on the same page, it's important that they feel guided, consulted and empowered in the process.

Both parents and students should have a clear understanding of the 'why' behind the school's chosen device management strategy. That is, that the school is taking the necessary steps to provide a safe and productive learning environment for all students.

Have a clear course of action for breaches

Bypassing school filters needs to be taken seriously and dealt with according to school policies and behaviour management plans. Although monitoring student compliance does present yet another task on a teacher's plate, the risk posed to child safety and learning integrity is substantial and therefore can't go unactioned. Ensure that staff have a clear understanding of the steps that they should take when they encounter this behaviour and are properly supported in doing so.

Use technology to help identify and respond

It is important to have a comprehensive online safety solution for your school network that provides protection and visibility regarding filter avoidance behaviour.

Technology is available to prevent hotspotting and block the use of VPNs, which is important as it will help prevent distraction and minimise risk. However, as this is a behavioural issue, schools need to identify students demonstrating this behaviour to guide positive technology use. Talk with your IT team to understand which students are being blocked most frequently for VPN use and then implement your pastoral care team to help address the behaviour.

Ask your IT team to look at how often students are on the school network and how much data they use over an extended period, compared to their peers. A student using significantly less data on the school network than peers from the same year group is a strong indication that they are not using the school network to access online content.

The key is to use the tools you have at your disposal to provide evidence of where any problems sit, so you can implement a clear course of action for breaches of school policies.

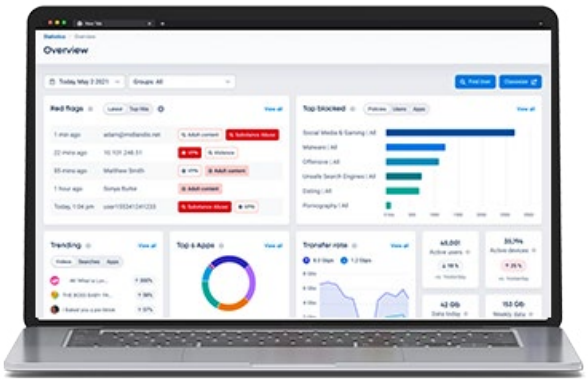
It's important to have a comprehensive online safety solution for your school network that provides **protection and visibility** regarding filter avoidance behaviour.

How Linewize Can Help Manage Filter Avoidance at Your School

Positively guide student online behaviour

Linewize School Manager provides real-time visibility and control over unwanted VPN activity on your network. Through a combination of proactive, human categorisation of VPNs and machine learning technologies, School Manager can swiftly detect, block, and report on VPN use on your school network. Having visibility of students employing VPNs empowers your staff to address the behaviour with students directly.

The Quarantine feature allows you to apply consequences for repeat filter avoidance, discouraging future transgressions and helping guide those students towards positive internet usage.



Educate and empower parents & families

Student time online is not just limited to time spent at school. Achieving positive online behaviour requires guidance, no matter where they are. The solution is a whole-school community approach to online safety.

Designed specifically to drive parental engagement, Linewize Community helps ensure your parents are involved in their child's online activity and empowers them to effectively manage online safety. Your entire school community is further benefited by education and guidance from online safety experts and the support of our dedicated Education & Engagement Team.

> Linewize offers a granular solution, not a one size fits all."

Russell Burt
Principal, Point England School

Linewize is the leading provider of digital safeguarding solutions in Australia. For more information, visit our website or get in touch with our team of experts.

Web: www.linewize.io
Email: sales@linewize.io

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