International Schools Partnership

Dear Parents,

Our Technology & Safeguarding teams are always trying to make things safer online. We looked at new tools to help us do this better. After testing these tools at one school, we decided to use Smoothwall's Monitor and Filter products for all our schools. This decision comes from the ISP head office in the UK and is for every school in ISP.

What is Smoothwall Monitor?

Smoothwall Monitor is a real-time, proactive digital monitoring solution that alerts safeguarding teams to activity of risk on school owned devices only in the school computer suite.

Works Online & Offline

Smoothwall Proactive Monitor helps find possible dangers not just from web browsing. It looks at what students do online, catching risky actions anywhere. This tool records what is typed, both online and offline. It works in regular web browsers, chat apps, and programs like Microsoft Word. It can even detect activities in secure, hidden web browsers

Works in realtime

This service has real people watching over it 24/7, every day of the year. It captures activities as they occur and checks them instantly. If there's any sign of danger, it automatically gets marked for a human to look over. This person double-checks to remove any mistakes, saving you time from going through data. This way, you can focus more on teaching and learning.

Immediate safeguarding alerts

Acting early can help students do better. If there's a big risk, it's quickly reported to your safety team by phone and email. This fast response can make a big difference for students.

Where confidence grows

How does Smoothwall Monitor works?

Students types into device - Keystroke are logged even if deleted

At risk words or behaviors are identified

Artificial Intelligence assesses & sorts by risk level

Incidents of all risks levels are recorded in dashboard

Potentially high risk incidents are also passed to human expert moderators for reviews

Where needed, school Digital Safeguarding Leads (DSLs) are alerted immediately by phone/email

Where confidence grows

What is Smoothwall Filter?

Smoothwall Filter provides device based, real-time content-aware analysis. It scans the copy, content, and context of every web page for unwanted material and has 120 filtering categories which can be used to tailor the web browsing experience of all audiences to ensure that harmful content is out of reach. We kindly encourage all students to equip their study devices with Smoothwall. It's an important addition that significantly contributes to enhancing student safety and safeguarding.

Key Features

The intelligent web filter sorts new and existing web pages correctly as they come up. It does this by looking closely at the content, the situation it's used in, and how each page is put together, all in real time.

The built-in safety reporting system alerts you to any safety risks, covering 7 categories including radicalization, suicide, and self-harm.

This system does more than just block websites. It offers tools that let you see social media without making changes and remove any unsuitable content from these sites.

Create custom rules depending on the group of users, time, place, IP address, network segment, and device names for mobile devices and laptops.

Find and block harmful or malicious content and filter web traffic that is protected by Secure Socket Layer (SSL), including secure hidden proxy services.

Where confidence grows

Frequently Asked Questions for Smoothwall Filter on student owned devices

Q: Is Smoothwall Filter loaded onto all student owned devices?
A: We kindly encourage all students to equip their study devices with Smoothwall Filter. It's an important addition that significantly contributes to enhancing student safety and safeguarding.

Q: Does Smoothwall Filter work across all devices? Chromebooks, Apple etc?
A: Yes, the system works just as well on Windows, Apple as we do on Chromebooks.

Q: What written languages does the software detect?
A: English and Spanish are fully supported by the software. Other languages are supported and ongoing moderation of these improves over time.

Q: Is the Smoothwall Filter system able to recognise pictures or monitor voice inputs?
A: Smoothwall currently captures images based on typed keystrokes, with our moderation team reviewing on-screen activity. If a trigger occurs, they assess the context and identify any inappropriate content. We are actively developing more features, including image recognition. Currently, voice conversations aren't monitored, but audio monitoring is part of Smoothwall's future plans.

Q: Will Smoothwall Filter capture and harvest personal data, things like passwords or bank account details?
A: No, Smoothwall is designed with privacy and data protection in mind, not for data scraping. It operates on specific triggers, avoiding unnecessary data areas and using blanket blocks to filter out false positives like secure sites (e.g., hsbc.com). Our focus is on safeguarding, with global and countrywide Data Protection Officers ensuring that sensitive information, such as passwords and bank account details, is always excluded from monitoring.

Q: Can students can get around the monitoring by using a VPN or their own personal hotspot?

A: They may well be able to get around the filter aspect but Smoothwall Filter works in a different way, it is looking at what keystrokes happens, so whether you're on a VPN or a hotspot or you're on Windows application or a Google application, it's looking at what's happening as it's being typed in, regardless of the application, or whether there's a VPN or hotspot.

Q: How can I be sure any safeguarding concerns are safe and confidential?

A: Schools sites are fully contained in one place with safeguarding alerts only available to pre-defined DSL's. The ownership of the data remains with the school. Think of this as a digital version of in person safeguarding.

Q: Can the school identify which specific device is being used?

A: Yes, because it registers each individual device, so we can see identify which device was being at what time. In the data you will be able to access in the events tab, this shows you the name of the user. It shows you the device that it was done on, so it would be able to differentiate at that point.

Where confidence grows