Impero

The Students' Voice Survey:

Safer Internet, Stronger Learning Outcomes

www.imperosoftware.com

Contents

Victoria Raynor

International Safeguarding Consultant and Trainer DFIFIP
Co-founder & Director Schools Like Us

Victoria Raynor is a strategic leader in Safeguarding in Education and is dedicated to driving change and improving outcomes for children and young people.

With nearly 20 years of experience, Victoria has developed a deep understanding of the complex challenges involved in safeguarding in education and honed her skills in developing and implementing effective strategies to address them.

2,000+

Impero surveyed students to better understand their perspective.

Foreword by Victoria Raynor

How schools can improve online safeguarding with sophisticated software solutions.

Helping children navigate today's online world is an increasingly difficult challenge for teachers and parents. Keeping up with the constant stream of new developments can feel impossible, but it's essential – especially as many of today's 11-18-year-olds are likely to build successful, tech-driven careers we've not yet heard of. As they go through secondary education, students need access to trusted, informative online content that will help them reach their full potential.

Yet they also need to be safe. Cases of cyberbullying and stalking, online scams, misuse or stealing of personal information and images, gambling, and accessing inappropriate or harmful content are increasing among pupils, and schools have a duty to protect students from these threats.

The debate continues to rage over banning phones and devices in schools. Many schools have opted not to allow any personal devices at all, yet pupils are still accessing prohibited content and social media (and being targeted by others) on school devices. So, what's the solution?

To help answer that question, at Impero, we surveyed more than 2,000 secondary school children aged between 11 and 18 about their use of mobile phones and other Internet-connected devices, inside and outside school, including during lesson time, and on personal and school-owned technology.

The findings are both eye-opening and concerning, and point to a need for intelligent, balanced safeguarding solutions tailored to pupils' requirements across different ages when it comes to managing devices in school. This includes, fundamentally, a specialised system for Internet filtering and monitoring, along with classroom management and student wellbeing monitoring tools that will help protect against online threats, while facilitating learning during this pivotal period of education.

Read on to learn more about our findings – and to discover our five key recommendations for fortifying online safeguarding in your school or multi-academy trust.

1. Build a safeguarding-centric approach with flexibility.
2. Create integrated safeguarding solutions.
3. Establish comprehensive filtering.
4. Produce customized reporting for stakeholders.
5. Ensure universal compatibility.

11-18

Age group likely to build tech- driven careers we're still unaware of.

70%

Believe there is room for improving online safety.

Digital Natives

Examining online behaviours and device-use in schools.

The digital landscape has transformed the way today's students interact with the world. They are digital natives: to them, the use of personal devices and laptops, social media and the internet comes as second nature. But while this has offered huge potential for learning opportunities, it has also created significant challenges for safeguarding in schools. Through our survey we've been able to probe more closely some of these challenges - such as the extent to which children are using social media platforms at an earlier age than they're supposed to, and the numbers of students who understand terms such as "dark web" and "deep fake". Here we break down some of the key statistics.

Early Engagement with Social Media

Most social media platforms require users to be at least 13 to sign up for an account, while WhatsApp is rated 16+. But our research reveals that this isn't stopping students from becoming active on social media before these recommended ages.

For instance:

97% of students joined WhatsApp before the age of 16.
72% started YouTube channels before they turned 13.
53% opened a Snapchat account before 13.
43% created an Instagram account before 13.
43% joined Facebook before the age of 13.

There were also large numbers of early engagers for the likes of Twitch, Telegram and Twitter. This suggests – very strongly – that most students aren't waiting until the recommended age to sign up for social platforms, potentially accessing age-inappropriate content from an early age.

Understanding Online Concepts

A striking trend among students is a growing awareness of online concepts that can be in some respects difficult, mature or perhaps even illegal.

We can see this from the fact that:

56% are aware of the dark web.

54% know about generative AI.

40% are aware of social engineering.

39% grasp the concept of deep fake.

This represents a double-edged sword. While this familiarity could be useful in helping students navigate online threats, it also exposes them to complex risks at a comparatively young age.

97%

Joined WhatsApp before age 16.

70%

Started YouTube channels before age 13.

39%

Grasp the concept of deep fake.

Digital Natives

Examining online behaviours and device-use in schools.

Device Use

More and more students are bringing their own personal devices to school, as well as using school-managed devices. But while students are often using these Internet-connected devices at school to enhance their learning, our research highlights that they're also being used in ways that might cause concern:

50% of students used devices to access social media.

38% have played online games during lessons.

24% have filmed others without permission.

24% have viewed harmful or violent content.

20% of students have accessed the dark web.

13% have visited X-rated websites.

10% have accessed gambling platforms. Additionally, more than a quarter of students, **27%** have successfully circumnavigated' the school's Internet filtering system. This is an indication that many students have become more adept at using sophisticated tools such as VPNs or proxy servers to circumvent filtering systems.

This is particularly worrying, considering that a school should have complete confidence that its Internet filtering system is robust enough to prevent all students from circumvention. And with the increasing number of personal devices brought to school, the filtering system must be able to control Internet access from these devices, too. To aid with awareness, schools must have clearly defined policies on device usage, including school-managed devices and personal devices brought in by students from home.

The widespread use of Internet-connected devices in schools presents both opportunities and challenges, as shown by this data. Many of the positive uses, such as widening the scope and potential of learning, are balanced by concerns over what they're used for alternatively, including early and disruptive social media use, and filming or taking photos without permission. Ultimately, balancing risk mitigation with responsible digital citizenship is essential, all underscored by reliable tech-driven safeguarding solutions. And that will come from effective collaboration between schools and parents, who will need to play a critical role in fostering digital literacy and safe online practices at home.

50%

Students use school devices to access social media.

38%

Play online games durring lessons.

13%

Accessed x-rated websites.

External Threats

The top safeguarding concerns for schools.

In our digital age, schools face a massive array of online safeguarding threats posing risks to students inside and outside the premises. As these threats become increasingly diverse, complex and difficult to avoid, schools must adopt sophisticated solutions for Internet filtering, classroom management and student wellbeing monitoring.

According to our survey, a significant percentage of students have already encountered a host of online safeguarding threats. These include:

Cyberbullying and Harassment

Up to **37%** of students have experienced harassment or cyberbullying at some point during their time at school. Equally as worrying, **20%** have been approached by online predators.

Online Scams and Gambling

Our survey found that **41%** of students have encountered online scams at one time or another, while **45%** have been asked to engage in games or gambling with their money. These figures highlight the potential financial risks and pressures facing students.

Data Privacy

A growing problem, **15%** of students reported having their personal information or images leaked, misused, or stolen.

Inappropriate Content Exposure

The survey also shed light on the frequency with which students encounter inappropriate content on their devices - often through ads or web pop-ups - without actively looking for it.

This issue is showing no signs of going away soon. In fact, **60%** of students believe it's becoming increasingly difficult to avoid coming across inappropriate or harmful content online.

37%

Experienced cyberbullying or other types of harassment.

60%

Feel it's becoming more difficult to avoid harmful content.

20%

Approached by online predators.

79%

Exposed to offensive language and images.

The Right Balance

Ensuring Internet safety without restricting learning platforms.

Students need to be able to use devices at school: they are vital tools for enhancing learning. But schools need to guarantee a positive and safe online learning environment for students, while empowering them with the digital tools they need. It's a difficult balance to achieve, and at the moment the measures put in place by schools paint a mixed picture.

Device and Content Bans

According to our survey, gaming devices top the list as the most commonly excluded, with **64%** of students saying they're prohibited in their school, while **48%** reported a ban on personal laptops and tablets. Amidst government plans to introduce a nationwide blanket ban on mobile phones, **46%** of students said their school already has such a policy in place. Interestingly, however, only **36%** of students agreed that personal student devices should be banned, exposing a disparity between school policies and student opinions.

Web-Access Challenges

Ensuring access to useful learning websites can be challenging, as 31% of students face regular blocks in their attempts to access them. Older students, particularly those aged 18, seem to encounter more frequent obstacles, with **44%** experiencing access issues. This can have serious knock-on effects, with students who are doing GCSEs or A-Levels potentially needing ready access to websites that might be blocked due to a lack of age-sensitive filtering.

This is borne out in the results of the survey, where **70%** of students believe there is room for improvement in striking the right balance between online safety and access to educational content. A majority of students **(52%)** express the view that Internet filtering should be more flexible and tailored to different age groups. This indicates a desire for a nuanced approach that considers individual needs and developmental stages. Specifically, this would mean adopting Internet filtering based on digital ID, which would grant students access to certain sites depending on the age or year group of the student using them.

Perception of Platforms

Knowing what kind of websites to block also complicates the creation of this ideal balance, with some surprising online platforms being used as valuable learning resources.

Take YouTube for example, which was cited by **90%** of the students we surveyed as a valuable resource for learning, while TikTok was given a tick by over half, **53%**. This is despite almost half saying that their school prohibits social media use on any type of device. Meanwhile **30%** of students said they find the AI-driven ChatGPT to be beneficial.

In these cases, it's the content itself which needs to be managed, rather than necessarily the whole site. So any age-restricted content on YouTube, for instance, can be filtered, while other content remains accessible.

Student Involvement

Nearly half of the students we surveyed **(49%**) said they thought students should have more say in determining which sites are blocked, while a significant proportion of students **(45%)** perceive their families as being stricter about online safety compared to their schools, and only **23%** hold the opposite view. This implies that schools might benefit from aligning their policies more closely with the vigilance exercised at home.

Ensuring a safe online learning environment, while providing access to valuable learning platforms, requires a careful balance between Internet safety and flexibility. By taking student needs into account, schools can refine their approach to Internet filtering.

44%

Experience web access issues.

Unlocking Potential

Five key recommendations for effective internet filtering in schools.

As the new academic year gets under way, **Sam Heiney, SVP Strategy and Product Marketing at Impero** shares five tips for implementing an effective internet filtering system in your school.

1. Build a Safeguarding-Centric Approach

In accordance with the Keeping Children Safe in Education (KCSiE) guidance, internet filtering should be viewed primarily as a safeguarding solution, focusing on student wellbeing rather than just an IT measure. Leverage digital IDs to tailor filtering based on age groups and specific educational needs. This approach allows for more flexibility while maintaining a strong safety net.

2. Create Integrated Safeguarding Solutions

Develop an integrated stack of safeguarding solutions that includes internet filtering, monitoring, student wellbeing reporting, classroom management, and secure remote device access. By concentrating on the free-flow of data between these systems, it will help create a more holistic view of student safeguarding across different tools. Having this fuller picture then enables early intervention in potential safeguarding concerns.

3. Establish Comprehensive Filtering

Ensure robust internet filtering for all devices, including personal ones, while connected to the school network. Take regional requirements into account, such as blocking specific regional sites and detecting region-specific keywords or slang to address local concerns effectively.

4. Produce Customized Reporting for Stakeholders

Tailor the types of reports generated by your internet filtering system to suit different school stakeholders' needs. For instance, safeguarding leads might require reports on visited sites, IT teams may need network performance insights, and school leaders and administrators might want reports that provide an overarching view of online safety.

5. Ensure Universal Compatibility

Make sure your internet filtering system is compatible with all types of internet-connected devices commonly used in schools, and that it works with older models, so you support access to online safety measures for all students.

Case in Point

Frenship ISD uses AppDefender, a tool within ContentKeeper, to detect and block rogue apps used to circumvent web filters.

In this district of 10,000 students it was common to see 400-500 suspicious apps identified. A large number of students used free tunneling apps to bypass the district's filtering software, often so they can play computer games during school hours.

Whereas the district's firewall failed to block these rogue apps, ContentKeeper succeeded. As a result, students are now being kept on task far more effectively as they use Chromebooks and other digital devices for learning—and precious bandwidth is no longer being wasted on gaming, VPN and other non-sanctioned activities.

ContentKeeper

"How can we efficiently utilize district resources while providing a safe secure learning environment? ContentKeeper App Defender helps us do this is in a very effective way."
-Joe Barnett , Frenship ISD
Chief Technology Officer

Additional Information

Resources

Wellbeing
Support for mental health

Our new Wellbeing Hub offers you access to tools, information and support for your proactive strategies.

Visit the hub

Safety
Beyond filtering

Behavioral Intent Alerting for comprehensive Reporting and Analytics solution to keep students safe.

Access whitepaper

Technical
Support for IT teams

Access our new buyers guide to help support your content filter, safeguarding and wellbeing needs.

Access the guide

About Impero

Since 2002 Impero has worked with schools across the globe, on a mission to keep students safe and productive in a digital learning environment. Impero has a suite of software solutions to address classroom management, student wellbeing and remote device control in education, and is a well-regarded name in the EdTech space. In early 2021, Impero acquired **ContentKeeper,** a leading web filtering solution, specifically designed for the unique requirements of education. With granular controls and detailed reporting, across all device types, ContentKeeper has become a core component in Impero's product portfolio.

UK

+44 (0) 1509 611 341

Seventh Floor,
East West Tollhouse Hill,
Nottingham, UK NG1 5FS

US

+1 844-346-7376

10300 SW Greenburg Rd, Suite 303,
Portland, OR 97223

Email

Sales: sales@imperosoftware.com
Support: support@imperosoftware.com
Press: press@imperosoftware.co.uk