

# Safeguarding students online

Safer Internet Day, held last week, is a global initiative that aims to promote safer and more responsible use of online technology and mobile phones, especially among children and young people across the world. This year's theme is 'Play your part for a better internet'.



©Artisticco LLC via [123RF](#)

Google SA offers the following tips and techniques that schools can follow to make their online spaces safer.

As we move further into the digital age, more schools are adopting a digital approach to education. This inevitably means getting their students online, and using tools and devices that enable learning in this new environment. Institutions like schools are obligated to take appropriate measures to help protect their students from the potential dangers of the internet, such as inappropriate content, malware, privacy threats, and so on.

Protection of students is complicated when it comes to the internet. It is challenging even for parents to control what learners may or may not engage with on public domains. However, schools may be able to effectively police their own networks, if properly set up, and strategised.

A structured orientation course taught at the start of every school year should familiarise each student with the proper use and protocols for the school network. Much as a parent might construct an agreement with internet use for their child, the

school may also opt for a set of rules agreed upon with students. This would include some guidelines on what potential threats to be aware of, what to do in case of cyberbullying, and so on.

In addition, more schools are drafting a specific policy around whether or not students and teachers are allowed to use their own devices on the school network. Laptops and tablets may be secure at school, but because users are likely to use them elsewhere, they could present malware or virus vulnerability down the line.

Moreover, while technologies exist to protect these devices even while they are not on the school's network, being vigilant about upgrading the school's web filter will go a long way to sidestepping these kinds of problems. Cloud-based anti-malware protection, for example, has enabled far more flexibility when it comes to protecting information and networks.

Even Google's free Apps for Education (GAFE) service has recognised the value in cloud-based digital education tools. When learners have GAFE accounts set up through their school's domain, access to a number of tools, as well as email, shared resources and cloud drive space is given, within the limitations of a school's network. For example, the school might restrict use of the email only to others in the domain, meaning, email can only be sent to others who belong to the school.

Beyond that, networks are very flexible when it comes to controlling use, even down to restricting at which times students can log on. The key for schools and parents is to maintain open lines of communication, and to remain vigilant of the ever-evolving web.

For more, visit: <https://www.bizcommunity.com>