# THE RISK BUSINESS

**Among a school's many duties to its pupils and parents is the need to manage the potential risks inherent in accessing the internet from the ever proliferating number of devices on site. With critics lining up to castigate schools adopting draconian filtering approaches, what are the smart ways of handling this challenge?**

Written by: Dean Gurden

"When it comes to internet access in the school environment, the stupidest thing you can do is to block all the websites your pupils might go to. Your philosophy should be to educate, not to ban." So says Paul Spencer-Ellis, headmaster at Royal Alexandra & Albert School, a state boarding school in Surrey. Thankfully, it's a view that's gaining increasing traction in teaching circles.

Not that there aren't a host of potential risks for pupils using technology and accessing the internet within a school environment. The point is that banning or blocking access to every website is simply a non-starter in the 21st century. So how do schools go about achieving a balance between allowing pupils to access the internet to facilitate learning, and blocking or

filtering potentially harmful sites?

Firstly, let's establish some of the main risks involved. Childnet International, a registered charity established in 1995 that works with a range of concerned parties to help make the internet a safe place for children, encapsulates the risks with its 'three Cs'. The first is 'contact', which involves anything from grooming to cyberbullying. According to government figures, more than a third of children aged between 12 and 15 have been victims of cyberbullying. And although it tends to happen more often outside of school – where there's generally more freedom to use technology – it still has a direct impact on the lives of the pupils at a school.

Secondly, there's 'content', which includes pornography, illegal content, inaccurate information, and also user-generated content where children put up their own material about themselves. Thirdly, there's 'commercialism', which involves data protection, such as when children register for things online or enter competitions, often providing personal information. What then happens with this data? Will it be shared and will the pupils be vulnerable as a result?

**"If you don't allow children to get into the water, you can't teach them to swim"**

This final category also involves the issue of online advertising. Interestingly, Childnet undertook a study with the National Consumer Council at the end of 2007 where children were asked if they knew what an online advert actually is? Surprisingly, and a little worryingly, a great many of the children replied that it was only an advert if it moved, opening them up to the murky world of stealth advertising.

Listed in this fashion, it's a worrying catalogue of things that can threaten pupils online, but a knee-jerk reaction of banning access to everything plainly doesn't work. If Spencer-Ellis' opening statement wasn't enough, he is happy to go further: "If you look at history, prohibition didn't work; saying that children can't buy alcohol under the age of 18 doesn't work, and saying to children you cannot access certain websites doesn't work. Any 14-year-old worth their salt will show you how to get around blocking software. It's also just not an intelligent approach, in terms of education, to say 'don't do this'. As human beings, if we're told we can't do something, it simply arouses our curiosity. Yes, we have filtered internet access at my school, but if you want a lesson on how to get around it, I'll get Gareth to show you – he's 12 years old.'

It's a point of view backed up by Ruth Hammond, manager, Safeguarding Programmes, at Becta, who also represents Becta on the Home Secretary's Taskforce on Child Protection on the Internet. "If schools are not allowing these technologies into the school to facilitate learning, then the kids are missing out on their potential benefits," she says. "We're steadily moving away from the idea of a lockdown approach to managing behaviour and risk. To use a simple analogy, if you don't allow children to get into the water, you can't teach them to swim."

Spencer-Ellis at the Royal Alexandra & Albert School cites an interesting example of the downside of blocking software – his school uses a monitoring system from >

Paul Spencer-Ellis, headmaster at Royal Alexandra & Albert School

Royal Alexandra & Albert School

**"We're concentrating on educating children in the responsible use of the internet"**

Securus. Following installation, Securus automatically flagged up the use of the F-word, suddenly appearing hundreds of times across the school's network. Further investigation revealed it to be a pupil doing research for GCSE English Literature, perusing the lyrics of various rap artists in the process. "Under those circumstances, although it's not language I'd encourage them to use, it's fine," says Spencer-Ellis. "But a simple filter system or blocking system would have removed the F-word or denied access to the site altogether, and we're aware the situation is more complicated than that. So although we have a filter system, we don't spend hours modifying or working on it, as there are websites appearing every second. Instead, we're concentrating on educating the children in the responsible use of the internet."

As you might expect, Becta offers guidance in this area. Hammond uses the acronym 'PIES' to deliver the published guidance on keeping pupils safe. Firstly, focus on 'policy': have a good acceptable use policy which is practised by everyone at the school. Have an 'infrastructure' which is as sound and secure as it can possibly be. Also 'educate' the whole school community as to what the risks are. And finally, S stands for 'standards': monitor to make sure your policy is updated, your infrastructure is still sound, and that all relevant education is meeting the needs of those concerned.

"I also recommend that there should be an e-safety coordinator in the school," adds Hammond, "and preferably not somebody from the ICT team, but more likely somebody in a senior management position; largely because I want schools to move away from the misunderstanding that ICT causes the security problems. The technology facilitates risk, but it isn't the cause of risk. It's more the behaviour of children and the teachers that is the main factor. So all Becta's guidance is about safeguarding children as a child protection issue and not as an ICT issue.

"Schools need to be educating kids in the way they use all sorts of technologies. So >

Will Gardner, chief executive of Childnet

even if they ban the likes of mobile phones or Bebo in schools, they should still be educating children in managing the risks associated with using those devices outside of school. It's a matter of educating for life," Hammond adds.

It's a point well made. Any child can shoplift, and some do, but most don't because of the moral education they have received from their parents and others. Similarly, the way forward with internet access is to educate pupils to make the right choices. Even if they make the wrong choice, getting caught can actually be a useful experience; it's part of the process of saying there are consequences to your actions, so please don't do it.

Parents have a huge role to play, but in the opinion of many teachers, they often fail in their responsibilities. "If a school allowed two or three kids unlimited access to the internet with no supervision and no filter system, then the school would be deemed grossly negligent," says Spencer-Ellis. "But what I've just described happens in thousands of teenagers' bedrooms every day of the week, yet that is regarded as normal. There is seemingly almost no market for filtering or monitoring software for home computers and I think the parents are well behind on this."

There has been a fair degree of finger-pointing in the past when it comes to taking responsibility for children's online safety, with people saying it's the parents' responsibility or industry's, or it's down to the ISPs. Most of those involved now admit it's about making sure everybody understands that there should be a collective responsibility.

Roger Davies, the ICT director at Queen Elizabeth School in Cumbria, recalls days past when most young children seemingly played outside relatively unsupervised. "Yes this obviously did happen, but you still had adults in the community who generally kept an eye on things. And that's what we should be trying to replicate in our schools. I'm continually trying to engage children in online safety through assemblies and lessons, and getting them to pass the message on to other children, and through this to build up a supportive environment. We're trying to tell them that we don't know everything; you probably know more than us, but let's talk about it because we're all learning."

It's an approach supported by Will Gardner, chief executive of Childnet, who says: "We did some work with the Department for Children Schools and Families in 2007/08 to provide guidance around preventing and responding to cyberbullying, and the general approach we now advocate is trying to build a whole school community approach to the issue, involving the heads, the governors, the teachers, other staff, pupils and, importantly, the parents as well. After all, the parents are often the ones providing the pupils with the technology to access the internet. And as soon as the pupils get out of school, they are going home and using a lot of these services, so it's really important that they learn how to use them safely and responsibly. We're also trying to reach the parents to help them educate and support their children."

According to David Miles, development director at the Family Online Safety Institute, the need for parental education is acute: "The problem is that a gap has opened up between the way children use technology, both at home and in school, and the way parents do. For most adults over the age of 30, their experience of using the internet is fundamentally a 90's experience. It's very much a productivity tool to them, using email and applications. But children have opened up the internet and driven the way it has been shaped over the last five years or so. And I think it partly accounts for the fact that when parents look at what their children are doing, they find it difficult to relate to."

Miles agrees with Spencer-Ellis about home filtering: "You'd also think parents would fit filtering software on to their children's devices," he says, "but the level of take-up is phenomenally low, and this has been the case for the last eight years or so. This isn't bad parenting, it's simply that the parents haven't used these devices in the same way as their children are doing, so they're not cognisant of the risks that their children are facing. And I genuinely think some teachers have a bit of this attitude as well, which can make it very challenging."

That attitude is changing though. Keeping pupils safe online is of paramount importance and schools are most definitely playing their part. Yet although this naturally means there is a place for content filtering, many schools are now wising up to the fact that this can't be the central plank of their risk management policy. The starting point has to be education. The way the Worldwide Web is shifting, each child in a developed country will have, as an adult, an online presence and you have to educate them to manage that safely and securely.

And ultimately, as Davies says: "Draconian filtering and locking things down is not protecting the children, it's merely protecting the institution." ICT