Playing it e-safe

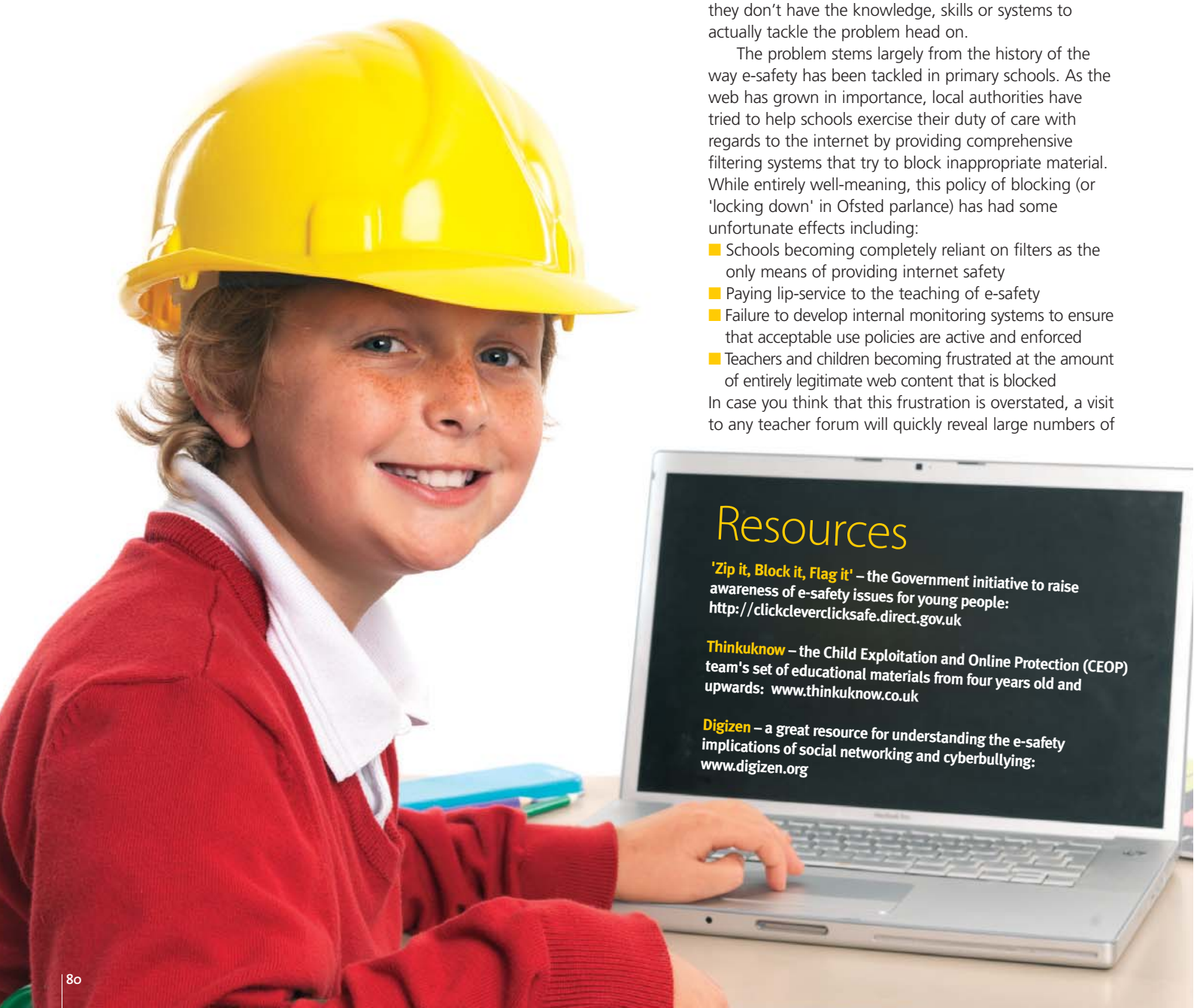
Taking responsibility for online security can benefit school and pupils alike, explains **John Sutton...**

Being in the privileged position of visiting lots of primary schools, I can say with a degree of confidence that most don't take e-safety seriously enough. That's not to say that they don't think it's a serious issue (far from it in my experience); it's just that they don't have the knowledge, skills or systems to actually tackle the problem head on.

The problem stems largely from the history of the way e-safety has been tackled in primary schools. As the web has grown in importance, local authorities have tried to help schools exercise their duty of care with regards to the internet by providing comprehensive filtering systems that try to block inappropriate material. While entirely well-meaning, this policy of blocking (or 'locking down' in Ofsted parlance) has had some unfortunate effects including:

- Schools becoming completely reliant on filters as the only means of providing internet safety
- Paying lip-service to the teaching of e-safety
- Failure to develop internal monitoring systems to ensure that acceptable use policies are active and enforced
- Teachers and children becoming frustrated at the amount of entirely legitimate web content that is blocked

In case you think that this frustration is overstated, a visit to any teacher forum will quickly reveal large numbers of



It's no longer sufficient to rely on external filters and to abdicate responsibility for e-safety by pushing it on to the local authority

discussions on the total lack of consistency of approach across the country. One authority I visited recently had bulk-purchased an expensive content system for all of its schools, and the filters in place had blocked all of the audio content in that system due to a blanket filter of mp3 audio files. Small wonder that the teachers there had virtually given up on the internet as a useful source of resources and learning tool: podcasting would be a bit of a challenge!

It doesn't have to be this way

At Becta's biennial conference on e-safety, 'Empowering children and young people in a digital world', I detected a wind of change blowing through the air. Most interesting was the presentation by Tanya Harber-Stuart, an HMI, who presented Ofsted's 2009 thematic study on e-safety in schools (see links). Ofsted visited 35 schools in various settings to get a snapshot of e-safety and found five to be outstanding, 16 good, 13 satisfactory and one unsatisfactory. All five outstanding schools were judged to be outstanding because they took a 'managed' view of e-safety – that is they proactively monitored their web connection and didn't simply rely on local authority filters to do their job.

Importantly, of the 13 schools judged to be satisfactory, all used a 'locked down' approach to e-safety (i.e. relied on an external filter), and Ofsted adjudged this to be, 'less effective in helping them to learn how to use new technologies safely', concluding that, 'These pupils were therefore more vulnerable overall.' The key message throughout the conference

Next steps

Taking real responsibility for e-safety in your school is not necessarily a scary or difficult task, but it does need thinking through and wide consultation. Take these four simple steps to move the e-safety agenda forward in your school:

1. **Adopt a robust and wide ranging acceptable use policy, consult widely and publicise its existence effectively.**
2. **Talk with your technology provider and make a plan to move to individual logins for all staff and children in your establishment (use a common password and aide memoire cards for early years and year 1).**
3. **Investigate and evaluate the means of providing an effective local web monitoring system either through the use of your existing cache box or by adding monitoring software and hardware.**
4. **Plan an Inset program for staff and an e-safety curriculum for children.**
5. **Most important of all, once implemented, evaluate the impact of your strategy – not just with the children, but with staff and parents too.**

seemed to be that it was no longer sufficient to rely on external filters and to abdicate responsibility for e-safety by pushing it on to the local authority, and schools need to develop a strategy for tackling the issue themselves. The report is freely available to download (see links) and makes for very interesting reading.

Where to begin?

There are some simple questions that could be asked of any school to reveal whether they have a 'managed' approach to e-safety:

- If you became aware of the accessing of inappropriate material on your web connection, would you be able to identify the individual responsible from evidence recorded by your network?
- Do all staff know the procedure to block/unblock a website?
- Is e-safety a planned element in your curriculum?
- Is there a named individual responsible for e-safety?

I have developed a simple questionnaire that highlights areas to think about when developing an e-safety strategy, and Becta has a useful free poster that will also help define a way forward (see links).

Taking personal responsibility

A fundamental part of my approach to e-safety is the importance of teaching children (and staff) about personal responsibility when using the internet. We don't teach children to swim with a video, and we can't expect children to take responsibility for their online behaviour if we don't provide an environment in which issues of e-safety can be safely explored.

I think that developing this sense of personal responsibility can be achieved in a number of different ways:

By developing an Acceptable Use Policy (AUP) that is shared and understood by the whole school community (see links for a sample policy).

Developing an AUP shouldn't necessarily be the job of the ICT coordinator. It should be one of the cornerstone policies for your school and may well include references to the use of personal ICT equipment (e.g. camera phones) by teachers; use of social networking sites by staff and children; what constitutes inappropriate content; and the use of ICT equipment off-site. For an excellent discussion paper that could be used as the basis of a staff meeting, see Kent Education's 'Safe Practice with Technology' document, and for a full discussion on the development of an AUP read my blog post on the subject (see links).

By developing a system where everyone has an individual login and everyone is taught the importance of password security.

Individual logins to your school network are an absolute fundamental of any e-safety monitoring system. Obviously if the whole class is using the same login, then no attempt to access inappropriate material can be pinned to an individual without witnesses. Having individual logins also helps children understand the importance of password security. Without the sense of the 'personal' that an individual login brings, any notion of taking responsibility for your own online behaviour is abstract.

By introducing a 'locked down' approach to filtering to a system which monitors web activity and proactively enforces the school's AUP.

Monitoring your own web connection isn't necessarily as difficult or time consuming as it sounds. Many schools have cache boxes as part of their local authority filtering solution, which usually contain software that allows schools to view reports of web activity as well as to block and unblock websites themselves. Often it is a case of getting some training in the use of the software on the box. If that's not possible, then consider implementing keystroke monitoring software (see case study and links for providers). This 'watches' every keystroke that a user makes and reports any potentially inappropriate language to the network administrator. If that sounds a little like 'Big Brother', then read the case study to understand how effective they can be.

By embedding e-safety in the culture of the school, through inset planned to meet the needs of staff and a PSHE curriculum incorporating e-safety.

The DCSF had decided to make e-safety education a compulsory part of the curriculum from September 2010. But even if this changes, there really is no excuse for not having e-safety as a planned part of your annual programme.

In the Ofsted report on e-safety, staff training was identified as the weak link across all schools: 'The weakest aspect of provision in the schools visited was the extent and quality of their training for staff. It did not involve all the staff and was not provided systematically. Even the schools that organised training for all their staff did not always monitor its impact systematically.' The message from Ofsted is clear.

Web Links

HEAD ONLINE FOR MORE INFORMATION ON E-SAFETY...

Ofsted's thematic study of e-safety: http://bit.ly/ofstedstudy
Sample AUP: http://bit.ly/sampleaup
Safer Internet Questionnaire: http://bit.ly/saferwebquestions
Becta e-safety poster: http://bit.ly/bectaposter
Blog post on developing an AUP: http://bit.ly/aupdiscussion
Becta discussion paper on developing an AUP: http://bit.ly/bectaaupdev
Kent LA: 'Safe Practice with Technology': http://bit.ly/kentsafetech

Case study: an AUP in action

A few years back we subscribed to a private broadband provider (www.inty.com) because the LA hadn't got their broadband up and running at the time. The filters were fairly liberal, but user control was excellent – we could block any site and ban any user very quickly. To back this up we used a piece of software called Policy Master, which monitored every web page pulled up, every email sent and every keystroke on every workstation. We knew, and had evidence of, every dodgy search term entered into the system and used the AUP to inform parents whenever we felt there was a deliberate attempt to access inappropriate material.

Crucially, because the children (and staff) knew that their web activity was monitored they did not attempt to abuse the system. In three years of daily monitoring I can only recall one instance of a deliberate attempt by a child to access porn. (Note: the monitoring was shared by three trained individuals and took, on average, less than five minutes per day).

Overwhelmingly, the policy violations were accidental, for example a dodgy word on a page of legitimate search results or an unexpected advert on a web page. But we recorded any deliberate violations in a log book with the follow up action noted (the AUP made it very clear that policy breaches by staff would be dealt with through normal disciplinary channels and that as ICT co-ordinator I had a duty to pass all breaches to the Headteacher).

WHAT WAS THE PRACTICAL EFFECT OF THIS SYSTEM?

1. We had a virtually open internet (it was a private connection, not LA) and we only blocked pornography and violence. This allowed teachers to use any tool that they felt they wanted to.
2. The AUP was a live and active policy. Breaches resulted in letters home, interviews with parents and consequences such as removal of login privileges for a period.
3. Children were trusted to use the internet in clubs, lessons etc. and developed a real understanding of the importance of keeping passwords private.

At first it felt a bit 'big brotherish', but I rapidly came to an alternative point of view – it allowed teachers to teach, children to gain trust and responsibility and school to demonstrate to parents how effective the school's Acceptable Use Policy was.

PROVIDERS OF MONITORING SOFTWARE INCLUDE:

Forensic Software: www.forensicsoftware.co.uk
Securus Software: www.securus-software.com
E-Safe Education: www.esafeeducation.co.uk