Keeping students safe online, while still allowing them to make the most of the educational opportunities offered by the internet, can be a tricky balancing act – Brian Evans and Teresa Hughes have some practical advice...

PROTECT & THRIVE

In November 2011, NSPCC research collated from Government reports found that 38% of young people had been affected by some form of cyberbullying. Ofsted has also warned that pupils are regularly accessing sites where they could potentially be exposed to grooming or abuse.

In January 2012, Ofsted recognised this as a serious issue and have placed e-safety at the heart of its ongoing inspection criteria. Since then, it has continued to judge the effectiveness of a school's ability to safeguard against online "bullying and harassment", monitor how consistently schools "manage pupil behaviour" and how they develop pupils' ability to "assess and manage risk appropriately and... keep themselves safe."

Despite this focus from Ofsted, cyberbullying remains a very real problem: just last month, a 15 year old schoolboy named Joshua Unsworth was discovered to have hanged himself at his home in Lancashire after enduring months of abusive messages on social networking site Ask.fm – a website that had already been linked to a number of teen suicides earlier this year.

Around the same time, a couple from Oxfordshire were sent to prison for grooming a 14-year-old school girl in an internet chat room and luring her to a hotel room in Manchester.

So, how can you ensure that your pupils are adequately educated and prepared to use the Internet responsibly? Here are some tips to make sure that pupils remain safe and refrain from unearthing malicious content without hindering the learning process:

Keeping your AUP up to date

First of all, it is important to establish and maintain an Acceptable Use Policy (AUP). This plays a key role in encouraging safe and responsible online behaviour. Rather than a strict list of 'dos' and 'don'ts', an AUP should be relevant to the circumstances in your school:

Involve your pupils in the process

If pupils feel involved in creating your AUP, they will be more likely to respect it and act upon it. Invite them to share their views and ask student representatives and school councils to contribute to your policies on e-safety.

Communicate your AUP effectively

Everyone needs to be aware of the AUP, including pupils, parents and teachers. Make sure parents and carers have a copy in their home-school agreement, so they can understand the rules and issues and reinforce the message at home. Your AUP should also form part of your staff induction programme.

Customise your AUP for different groups

Your AUP might be customised for different year groups or for students who have recently joined the school. Perhaps you want to remind staff about data security, using removable data devices securely or their professional conduct when they use social networking sites.

A Managed Approach

Schools have favoured a 'locked down' approach in the past, but blocking and filtering software alone is not sufficient to protect children whilst on the Internet, not least because most intelligent 14-year-olds can easily bypass blocked sites using a proxy server address.

Whilst such systems do contribute to an overall e-safety strategy, they do not flag bullying or grooming behaviour, nor do they alert teachers to the fact that students have attempted to access prohibited or worrying material, such as pro-suicide sites.

Ofsted has noted that 'managed systems', which have fewer inaccessible sites than 'locked down' systems, are more effective in helping pupils learn how to use new technologies safely. This is because they allow children to make mistakes in a safe online environment where they can get used to working within a defined set of boundaries. Blocking and filtering software can also have an adverse effect on children's learning by indiscriminately blocking potentially useful material.

A managed system allows teachers to monitor exactly what pupils are accessing and inputting at any point, enabling them not only to block malicious material but effectively educate students about relevant e-safety issues.

Educating the Educators

It is hugely important that teachers are up to speed with dangers posed to children whilst on the Internet. A 'one step ahead' approach is necessary to keep abreast of new gaming and social media sites, technical loopholes that pupils may look to exploit and manipulation tactics used by child groomers.

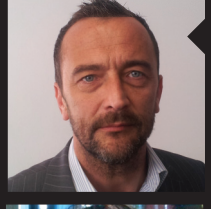
Organisations such as Beatbullying and the Child Exploitation & Online Protection (CEOP) Centre publish regular reports on their websites with the aim of keeping e-safety officers and teachers up-to-date with the latest e-safety guidance and concerns. It would be wise to take advantage of such resources by distributing them amongst your members of staff and perhaps condensing any appropriate information into a newsletter for your pupils.

Many managed service providers include a termly newsletter with their package that serves the same function as the aforementioned reports, as well as an ongoing support service to provide around the clock advice for teachers facing e-safety issues.

Responding Appropriately

Responding appropriately when things go wrong is vital:

- If you are concerned that one of your pupils is being groomed online, report it to the Child Exploitation and Online Protection (CEOP) Centre. If you believe someone to be in immediate danger, inform the police.
- Involve your school's child protection officer about any concerns at the earliest opportunity. If a pupil is involved, they may wish to inform child protection services.
- If the content is online, report it to the service provider. If it is on a social networking site, contact them directly and ask them to investigate urgently.
- If you suspect that illegal activity is being carried out on a school computer or that illegal material (such as indecent images of children) could be stored on the school system, also inform the police and the Internet Watch Foundation.
- If illegal content is found on the school's computer network, it's essential that no-one downloads, prints or emails it because this can be a criminal offence in itself. It is also important that the suspect computer is not touched or even turned on or off so that any evidence is preserved.
- With less severe instances of cyberbullying or the attempted access of harmful material, it is often appropriate to tackle the problem internally. It may be useful to turn the incident into a teaching opportunity by having a class discussion about the issue, the potential implications and how to safeguard against any future instances. This will also avoid any potential embarrassment or complications that can result from singling out pupils.



ABOUT THE EXPERTS

BRIAN EVANS IS ACCOUNT MANAGER AT REDSTOR, LEADING PROVIDER OF CLOUD SERVICES TO THE EDUCATION MARKET

TERESA HUGHES IS CHILD PROTECTION ADVISOR TO SECURUS SOFTWARE, A SAFEGUARDING TOOL WHICH PROTECTS PUPILS FROM A RANGE OF E-SAFETY THREATS, PROVIDE ESSENTIAL TIPS FOR IMPLEMENTING E-SAFETY WITHIN SCHOOLS