Issue Number: 2

What every teacher needs to know about e-safety

E-safety Support

What is e-safety?

- Ofsted defines e-safety as: 'The school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.' Three particular e-safety risks for inspections are: "Being exposed to illegal, inappropriate or harmful material, being subjected to harmful online interaction with other users, and personal online behaviour that increases the likelihood of, or causes, harm." Teachers need to be able to ensure that: "All groups of pupils feel safe at school (and) they understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe."

- E-safety is particularly relevant to ICT and PSHE, but it also permeates any subject or activity which makes use of the internet.

Why you, as a teacher, should be concerned about e-safety

All teachers have a duty of care to the pupils they teach. Teachers act 'in loco parentis' and are legally responsible for all aspects of pupil safety, including online safety, whilst in school. Any activity involving internet use needs to be carefully planned and assessed for risk to minimise the possibility of an e-safety incident.

All teachers need to be aware of:

- What e-safety in relation to teaching is.
- How to promote safe use of the internet in their own practice and in terms of expectations of pupil behaviour.
- What the latest trends are in children's' use of the internet and how to provide guidance in an age-appropriate manner.
- How to prevent e-safety incidents arising.
- What to do when an e-safety incident arises.
- The key websites used: to report e-safety concerns, such as http://ceop.police.uk; to report illegal pornographic obscene and content, such as http://www.iwf.org.uk/; and to offer appropriate advice to children, such as http://www.childline.org.uk.

Statistics about e-safety in schools

According to a recent NFER study (www.nfer.ac.uk/nfer/publications/95001/95001.pdf) on e-safety in schools:

- 18% of secondary teachers didn't believe or weren't sure if their school had an e-safety policy.
- 42% of teachers didn't believe that pupils had the skills to use the internet safely at home.
- 40% of secondary teachers weren't sure or didn't believe their school's e-safety policy was reviewed regularly.
- 46% of secondary teachers did not agree that they had received adequate e-safety training.
- 47% of secondary teachers were not aware or did not believe that their school had a dedicated e-safety coordinator.
- Only 47% of primary and secondary teachers believed their pupils were equipped with the knowledge and skills to report e-safety incidents online.
- 30 % of teachers were unsure or didn't know how to report e-safety incidents online.
- 75% of teachers across primary and secondary believed that mobile phones facilitated access to inappropriate internet sites during school time.
- 91% of secondary teachers reported that their pupils had experienced cyberbullying.
- **Ofsted expects 100% of primary and secondary teachers to be confident in dealing with and reporting e-safety incidents, and teaching e-safety effectively with measurable progress.**

© www.e-safetysupport.com 2014

E-safety in your teaching – what to watch out for

Teachers need to be aware of the latest trends in children's use of the internet – particularly in relation to your school and the children you teach. For example, which social networking platforms and blogging/questions/sharing websites are popular in your school? Local trends might not match national trends. In one school Facebook usage might be prevalent, in another Twitter might be predominant. Tumblr might dominate in one setting while ask.fm might be a craze elsewhere. Knowing what your children are using helps ensure your pastoral advice and e-safety planning can be pre-emptive. Knowing what could happen makes it easier to know how to prevent it happening.

Teacher's knowledge of e-safety should not just be limited to prevention strategies. If a child points out inappropriate, bullying or illegal content, teachers should be aware of the procedures to report and remove the offending content.

Firstly, this requires the teacher to be completely familiar with the school and/or LEA e-safety policy with regard to reporting incidents. Teachers need to be aware who to contact and how to preserve evidence, if required. Teachers, acting 'in loco parentis', also need to be aware of how a school can request removal of content, especially with social media websites such as Facebook.

Teachers need to become experts in offering age-appropriate advice and guidance to their classes, and parents, with regard to:

Unwanted internet contact:

- Preventing online grooming and teaching pupils how to report instances and remove any damaging content.
- Cyberbullying- how to avoid, prevent, and deal with instances of cyberbulling, and how to report and remove offensive material created as a result of cyberbullying.

Inappropriate internet content:

- How to avoid, report and delete content which may be: pornographic, illegal, obscene, violent or likely to incite racial or religious hatred.
- How to avoid and report content which encourages illegal or dangerous activity by pupils, or is simply age-inappropriate.
- How to set a good example with regard to downloading software safely, avoiding viruses, adhering to copyright law and knowing whether information is reliable and valid or not.

Privacy

- How to ensure social networking content stays private and doesn't end up in search results years later.
- How to ensure passwords are strong, password-protected information, such as banking details or parental online shopping details remain safe.
- How to prevent and deal with junk mail and spam, and also how to spot internet scams and 'phishing' emails and messages.
- Understanding how websites store and track data which might be used for valid marketing reasons, or abused to create spam or facilitate identity theft.

Mobile phones and devices

- Understanding how difficult it is to remove tracking data from mobile phones and how important it is to safeguard privacy on mobile devices – more so than on laptops or PCs.
- To be aware of high-cost premium-rate services, and the more general costs involved in operating a mobile device.

© www.e-safetysupport.com 2014

- Understanding how mobile chat services such as Skype or Apple Facetime work, what information is stored and logged, and why there is no such thing as 'anonymous' chat.

E-safety and professional conduct – why you should read your school's e-safety policy

E-safety and related policy forms and more general conduct guidelines produced by your school, LEA and GTC form part of your job description and working conditions in that in terms of professional standards, you are bound to follow the procedures or risk being liable for allegations of misconduct. In other words, every IT and e-safety policy and guideline your school produces is required to be read and adhered to by every teacher who works there. Any failure to follow any part of the policy might be used to formulate or support an allegation of misconduct, should an e-safety incident arise. Whether the e-safety incident is related to a pupil, or actions by a teacher, if the teacher does not follow, or was not aware, of the school's policies, their actions as a result might be grounds for misconduct.

In particular, teachers must be completely conversant and aware of:

- Acceptable use policies and agreements
- E-safety policies
- Social media policies
- School network and ICT equipment policies
- Data protection policies
- GTCE code of conduct (still referred to in many job specifications: http://dera.ioe.ac.uk/8257/)
- GTCS code of conduct - http://www.gtcs.org.uk/web/FILES/teacher-regulation/copac-0412.pdf
- GTCW code of conduct - http://www.gtcw.org.uk/gtcw/images/stories/downloads/professional_standards/GTCW_Professional_Code.pdf

E-safety in your personal life – ensuring your web habits at home don't impact on your reputation at school.

Avoid using a school laptop or your school internet access for personal reasons. Why? Because it will reflect your internet usage, whether appropriate or inappropriate, in subtle and often difficult to control ways. For example, your browsing habits are stored in cookies, traffic data, logs and profile archives. Due to the security settings applied to school laptops and school network accounts, you probably won't have the facility to delete cookies, or browse without cookies. Even if you click the "do not track" button on websites, the security settings applied by your school IT department will probably cause all data to be tracked.

Trackable data is used on every social media site, every search engine and many websites for advertising and demographic data. So if you browsed for washing machine price comparisons on your school laptop at the weekend, it's highly likely Google will serve adverts for washing machines in your History lesson on Monday. Similarly if you searched for holidays, jobs or beauty treatments, they will appear as adverts too. If inappropriate content was searched for – that might appear.

Similarly, 'suggested searches', pop-ups, search engine 'auto-complete' fields and targeted news can also prove embarrassing when it reflects out-of-classroom internet habits.

The way to avoid this is simple – don't use a work account for personal browsing. The teacher's use of the internet has to set a good example to the pupils.

© www.e-safetysupport.com 2014

Case studies

Downloading software without taking appropriate precautions

One teacher downloaded an application from the internet to illustrate a teaching point to a class using the computer suite and IT network. The software was installed without the knowledge of the IT manager, and via a memory stick, without being virus-tested first.

While the motive and reasoning behind using the software was completely honourable, the lack of thought with regard to checking the application for viruses led to an e-safety incident. The application – a screensaver creator – was not infected, but the documentation manual – a pdf file – was infected with a virus which caused a piece of malicious code to be installed on that particular workstation on start-up.

The code allowed the workstation, which was frequently switched on all day, to send a continuous stream of referred spam email from sources in Russia and Brazil to email addresses all over the world. Much of the email, while not visible to any of the staff or students at the school, did contain inappropriate material including adverts for sexual dysfunction medication.

The first the school knew about the incident was when the internet service provider abruptly suspended the school's account after tracing the source of the spam email – resulting in email and internet provision being removed. The school's IT manager traced the particular workstation sending the spam email and removed the malware, but not before the school had been without internet and email provision for five days. The school had to agree to an undertaking that this type of incident would not occur again, placing the school's ISP AUP agreement and contract at risk.

This type of incident can be prevented by only allowing authorised IT staff to install software on school networks.

Pop-ups on personal laptop.

One teacher used their personal laptop for teaching in the classroom and connecting to the IWB. During the previous weekend, the teacher has used a perfectly respectable gambling website to bet on the outcome of a football match. Unfortunately, the website installed an add-on which caused pop ups advertising gambling odds and promotions to appear every time a search result featured the name or location of a football team. For example, if the search page featured 'London' in the results, betting advertisements would pop up for matches involving Chelsea.

While this might have been irritating but not inappropriate at home, when these pop-ups appeared on the IWB during lessons when Google was used to find information, the content was deemed inappropriate. It also proved difficult to track down and remove the add-on from the browser to prevent any reoccurrence.

© www.e-safetysupport.com 2014

It is worth bearing in mind that many gambling, shopping, medication and pornographic websites use similar technology to employ unwanted pop-ups when using an internet browser. At home, this might present an annoyance, but at school, with a class of 30 students, such a pop-up could lead to a significant breach of e-safety.

This type of problem can be avoided by not using personal laptops or computer equipment for school use - and vice versa - not using school equipment or network profiles for personal browsing use.

Conclusion

E-safety is required knowledge for all registered teachers. Ofsted expects all teachers to be confident delivering all aspects of the e-safety curriculum, and reflect good practice regarding internet usage as part of the professional standards determined by GTCs.

Teachers need to know what e-safety is, and what teaching it entails. They need to be able to act pre-emptively, preventatively and reactively, as well as being able to report incidents effectively, offer age-appropriate advice and guidance, deal with the effects of cyberbullying and incidents, and use 'in loco parentis' powers to remove the after-effects and unpleasant material caused by e-safety incidents.

Furthermore, teachers need to be aware that their own usage of school equipment needs to reflect the good practice and standards expected of the students. Pitfalls and problems created by using school accounts for personal usage need to be actively avoided.

© www.e-safetysupport.com 2014