



10 Steps to Keep Children Safe Online

ABSTRACT

Technology, in particular the Internet, has completely changed the way that we work, shop, play and learn. Classrooms around the world have been transformed as teachers who now have access to real-time information, immersive technologies and creative tools inspire and motivate their students. Blogs, podcasting and video sharing now provide real and authentic audience for children's work as well as a rich variety of new learning materials.

However, with this technology comes increased responsibility. It seems that every other week there is a high profile news story about the latest online fraud, virus outbreak, inappropriate content being hosted on popular websites or children at risk from on-line predators using the very tools that have so much potential for learning.

One of the biggest challenges that education professionals face is effectively striking the balance between delivering a safe online environment for young people that is not so restrictive it diminishes the obvious benefits. This means giving young people the information and skills they need to use the technology responsibly, taking advantage of any opportunities, managing their own safety and the safety of others and being able to deal with any risks that occur.

INTRODUCTION

Technology, in particular the Internet, has completely changed the way that we work, shop, play and learn. Classrooms around the world have been transformed as teachers who now have access to real-time information, immersive technologies and creative tools inspire and motivate their students. Blogs, podcasting and video sharing now provide real and authentic audience for children's work as well as a rich variety of new learning materials.

However, with this technology comes increased responsibility. It seems that every other week there is a high profile news story about the latest online fraud, virus outbreak, inappropriate content being hosted on popular websites or children at risk from on-line predators using the very tools that have so much potential for learning.

One of the biggest challenges that education professionals face is effectively striking the balance between delivering a safe online environment for young people that is not so restrictive it diminishes the obvious benefits. This means giving young people the information and skills they need to use the technology responsibly, taking advantage of any opportunities, managing their own safety and the safety of others and being able to deal with any risks that occur.

Here are some recent statistics:

- In Europe, 51% of teenagers say they use the Internet without supervision from their parents.
- In the UK, 23% of parents with children under 11 allow their kids to access the Internet without supervision at home.
- In the UK, 84% of girls aged 12-15 use the Internet to contact other people.
- 18% of children and young people who have access to the Internet have reported experiencing content which they found inappropriate or harmful.
- Over 55% of UK computer users have a Facebook account
- 36% of 15-24 year olds now have a smartphone.

Technology is only going to get more and more integrated into our lives but by taking a few simple steps we can ensure that our young people remain as safe as possible.

STEP 1

Training children and young people

Simply blocking children's access to the Internet in schools is not an effective way of keeping them safe. Young people need to be provided with balanced and clear information that gives them, with the right skills, knowledge and confidence so that they can use the Internet responsibly, be aware of and be able to manage associated on-line risks.

Social networking sites such as Facebook are very popular with young people and although many providers have taken steps over the past 12 months to improve privacy and eliminate some of the risks. We still have a power of work to do to make sure children use these sites responsibly and really understand how they work.

The responsible use of technology including on-line safety should be a key component of the curriculum. Education institutes should establish a Student Internet Acceptable Use Policy and make sure that young people understand what it means. Both the policy and the students should be regularly updated. Usage data and an ability to enforce the policy will also be necessary if you wish it to have real impact..

STEP 2

Training for teachers and during teacher training qualifications

With the use of technology now incorporated into modern day learning, it is necessary for teachers and support staff to understand and address the benefits and risks the Internet exposes to children and young people.

Teachers should receive regular and compulsory training on digital safety and responsible use. School inspection bodies, such as Ofsted (in England) have advised that in schools where provision for digital safety is outstanding, all the staff not just teachers, share responsibility for it.

Education providers should ensure that all staff receive ongoing training and have access to advice and policies on digital safety. In Scotland, some of this support, advice and material is available on-line inside Glow (The Scottish Schools Digital Network). Systematic and realistic ongoing monitoring of the Student Acceptable Use Policy should also be introduced along with training for staff to help the school community support young people by recognising and challenging suspicious behaviour.

STEP 3

Training for parents

The statistics at the start of this document show that 51% of teenagers in Europe say they use the Internet without supervision from their parents and 23% of parents in the UK allow children under 11 to access the Internet without supervision at home. Indeed, one of the biggest threats to young people is parental naivety, poor awareness and lack of confidence when it comes to understanding new technology.

Education providers should initiate training for parents and carers detailing the need to manage and understand their child's activities online and share the available resources. Resources include Childnet's Know IT All for Parents, Think U Know and MyGuide. They should also highlight their own e-safety guidelines and detail their procedures around issues such as cyber-bullying and the misuse of privately owned equipment outside school hours. Sharing their Student Acceptable Use Policy, and even asking parents to co-sign it with their children, is also a good way for parents to understand what the school is doing to keep their children safe online and what they could leverage in their own home.

Learning and Teaching Scotland has produced a video for parents (and teachers) and many local authorities in Scotland are now offering 'drop in' sessions for parents and carers to keep them up-to-date with emerging issues.



ZIP IT

Keep your personal stuff private and think about what you say and do online.



BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

STEP 4

Blocking inappropriate content

Although children don't necessarily go looking for harmful or inappropriate content, young people are naturally inquisitive and it is very possible that they could inadvertently view material from sites that promote racial or religious hatred, extreme violence, or illegal content, through popups, emails or instant messaging. Many say that Internet Service Providers need to do more to block access to Websites that encourage harmful behaviours, however blocking such content risks driving vulnerable young people to more dangerous sites.

While organisations such as the Internet Watch Foundation have made a significant impact on reducing certain types of content, education providers need to use technology that is dynamic, stays up to date and reliably blocks access to illegal content and content that children may not be emotionally ready for. At the same time, education providers need to signpost more vulnerable children to sites that host more responsible content and contain links to relevant support services.

More advanced Web filters allow students and staff to safely access much more of the great educational content that's available online. Ofsted recently stated that where schools had deployed these types of dynamic systems rather than locking down access to the Internet, students had a better knowledge and understanding on how to stay safe.

STEP 5

Reinforcement of the digital code

The UK Government recognises that children and young people need to be aware of the risks in the online world and how to manage such risk.

In 2010 various campaigns were introduced to promote online safety; one such campaign from The UK Council for Child Internet Safety (UKCCIS) was its 'Zip It, Block It, Flag It' digital code, advertised in print, online, TV, radio, and as posters in public areas near schools.

Another example is the 'Click Clever Click Safe' campaign, which is the cornerstone of the strategy to inform and educate children, young people, parents and carers on how to keep safe online. Education providers should leverage such public awareness campaigns, including Internet Safety Day, in their ongoing Internet access training programmes with students.

STEP 6

Utilise existing education resources on online safety

The inclusion of digital safety in the curriculum is only effective where high-quality, up-to-date materials, resources and training support it.

Education providers should leverage and utilise materials already available to support children and young people's online safety in schools. There is no point in re-inventing the wheel and great resources already include Know IT All For Primary and Know IT All for Secondary, Think U Know, Teachtoday, Digital literacy and e-safety, and TeachersTV. The responsibility for the production of these resources includes UKCCIS, the Training and Development Agency for Schools (TDA), Learning and Teaching Scotland, Childnet, Child Exploitation and Online Protection Centre (CEOP).

STEP 7

Ensure providers of Internet access are delivering on child e-safety

Ofsted recently noted that in an analysis of self-evaluation forms from a sample of schools, the proportion of schools providing sufficient evidence of their strategies for ensuring child Internet safety and responsible use was low, especially in primary schools. Schools surveyed rely heavily on external bodies, such as their local authority or external contractors, to provide a degree of security but schools rarely evaluated the quality of the support received.

Education providers need to understand their duty of care when it comes to Internet safety and responsible use. Effectiveness of their on-line safety messages, measures and interventions need to be evaluated even when they are delivered by an external agency.

STEP 8

Using YouTube safely in the Classroom

YouTube contains a great range of educational content but there is also a lot of inappropriate content. It is also not just video clips that may be offensive, educationally relevant videos can have associated links, targeting advertising and comments that are inappropriate for some audiences.

Google, who owns YouTube, recently introduced a 'Safety Mode' setting on YouTube that helps filter videos, hide user comments and censor offensive words. This move is a step in the right direction the feature can easily be turned off, re-exposing the associated risks.

Education providers need to use technology which helps them realise the educational benefits of YouTube and other media content in a safe and secure environment while protecting the most vulnerable. Some institutions have build a library of appropriate subject-related and age-verified YouTube content with related comments and media clips removed enabling teaching staff to utilise the education benefits of YouTube without any of the inherent risks or distractions.

STEP 9

Blocking Anonymous Proxies

Children and young people will continually try to buck authority and attempt to view sites they shouldn't thinking that adults are trying to spoil their fun. The use of anonymous proxies to bypass filtering technology is common with youngsters who want to access Facebook, gaming sites or MSN during the school day potentially disrupting their learning, inadvertently downloading viruses on to the school system and slowing the school network down due to the increase in traffic.

Any filtering solution should perform a live contextual analysis and categorisation of Web sites not listed in their URL database to determine whether it is a proxy site, so that the session can be shut down and ensure the ongoing safety of children whilst online.

STEP 10

Protecting resources from malware

Viruses, spyware, email phishing and scareware can attack computers through infected emails, which can cause huge problems for schools. A major issue for young people is having their confidential information stolen such as user names and passwords from social networking sites, etc.

To protect students when online, education providers need to stop Web nasties from entering their network, infecting their systems and gathering confidential information. A proactive, bi-directional real-time solution provides continuous protection 24/7 and is much better than relying on a database of known malware sites.

CONCLUSION

Despite the inherent risks and dangers, the Internet and other technologies are now central to the effective delivery of the education curriculum. However, schools in conjunction with central government agencies and other NGOs, need to continue to work together to progress the significant improvements in child e-safety that has taken place over the past few years.

Technology alone cannot solve the e-safety challenge but has to form part of an integrated approach that includes education, awareness and training for pupils, staff and parents.

ABOUT BLOXX

Headquartered in the UK with sales offices in Holland, the USA and Australia, Bloxx offers appliance-based web and email filtering for medium and large organisations in both the business and public sectors. Bloxx has achieved unrivalled sales growth year-on-year to become a leading web-filtering provider with an estimated 2.5 million+ users worldwide. Leading UK investment groups Archangel Investments Ltd and Braveheart Investment Group Plc have invested in Bloxx. For more information, visit <http://www.bloxx.com>.

USEFUL RESOURCES

The Byron Review, www.dcsf.gov.uk/byronreview/

Ofsted Report - School self-evaluation: a response to the Byron Review, www.ofsted.gov.uk/publications/080203

Ofsted Report - The safe use of technologies, www.ofsted.gov.uk/publications/090231

Becta, www.becta.org.uk

UK Council for Child Internet Safety (UKCCIS), www.dcsf.gov.uk/ukccis/

Click Clever Click Safe, www.clickcleverclicksafe.direct.gov.uk/

The Internet Watch Foundation, www.iwf.org.uk/

Child Exploitation and Online Protection Centre (CEOP), www.ceop.gov.uk/

Childnet International – Know it All, www.childnet-int.org/kia/

Get Safe Online, www.getsafeonline.org/

E-Victims, www.e-victims.org/

Bloxx, www.bloxx.com

To learn more about Bloxx technology, book in for an online demonstration at bloxx.com/demo, call +44 (0)1506 426 976 or email info@bloxx.com.

