Filtering misconceptions

Filtering - Addressing Misconceptions

Following the Prime Minister's request that "family friendly filters are to be applied across public Wi-Fi networks" (Cameron, 2013), it's great to see public Wi-Fi providers responding all in the name of keeping our younger users safer online. Also, it's great that all the big internet service providers now offer free parental control tools that work with every device in the home (see our video guides about how to set these up). In educational establishments, professionals have to consider their duty of care to the young people who attend and usually, the implications of this mean that a more comprehensive filtering solution will be in place with added restrictions to help protect younger users.

The one thing that we don't hear often enough when filtering is mentioned in politics or the media is the fact that it is only part of the answer to keeping young people safe online. Regular conversations about online safety both at school and home form the other essential component. A reliance on filtering alone can cause some or all of the following issues to arise:

- Limited access to useful resources
- A decreased resilience to risk online
- The encouragement of unsupervised access elsewhere
- A barrier to learning
- Unexplained access to graphic images

Interestingly, Ofsted have reported that schools who heavily block access to content find it to the detriment of their e-safety practice. In contrast, those professionals who see filtering as only one piece of the puzzle can find that filtering:

- Can provide report logs on content accessed potentially tracing back to an individual
- When used effectively, can form a positive part of e-safety practice and policy
- Can be used as an effective review tool to help give your establishment intelligence about the content that is being accessed on site.

With all this in mind, let's explore some of the common misconceptions that people have about filtering:

Filtering stops children accessing graphic images on search engines - False

This is one of the most common complaints school internet providers receive and can be prevented, to a certain extent, by the use of a moderated search engine such as www.swiggle.org.uk. The problem with images nowadays is that their respective web addresses (URL's) don't always contain anything offensive. Considering that's what the filter will be looking at, it's not really surprising that graphic thumbnails may appear. Let's work this through and think of the URL as a code. If this code contains a 'trigger' word or string of letters/ numbers e.g. 'porn' or 'xxx' then chances are it will be picked up by the setting's filter. However, if this code is just a random string of letters and/or numbers, the filter won't necessarily recognize it, resulting in the graphic content being shown.

Filtering stops cyberbullying - False

This is a common misunderstanding. We need to remember it's not the websites that are the issue here, it's the behaviour being displayed. By trying to block access to the sites where people are being abusive, we're not addressing the real problem. Furthermore, if a young person wants to access something they'll just find another way to and this won't necessarily be very safe. Also worth noting that, the Internet Watch Foundation's CAIC filtering list prevents access to illegal content only.

What they can't see online won't hurt them - False

To the contrary. Consider this - would you expect Usain Bolt to be able to win the Tour de France without receiving guidance from a cycling coach first? (I mean the yellow jersey not the green one!) In the same way that Bolt would be out of his comfort zone in this situation, children too are entering unchartered territory online. They need to understand the different areas of risk online before facing these in order to learn resilience. Some points to consider that can help you encourage resilience are:

- Considering the steps your establishment would take if a young person happened to access something inappropriate online.
- Whether the young people in your setting are aware of what to do if they stumble across unsuitable content.
- How young people in your setting are empowered to report any problems online should they arise.
- Whether the parents and carers have parental controls set on their home devices.

Filtering protects childhood innocence - False

Filtering can help prevent access to the most extreme content but is only part of the solution. It's the same old message, education is key and professionals working with children have a really important part to play in ensuring children understand what content might upset them and what they can do if they come across this.

If you need further advice or support with any incident relating to exposure of extreme content online in your setting, you can call the Professionals Online Safety Helpline on 0844 381 4772 or email them at helpline@saferinternet.org.uk