Giving staff and students access to the vast resources of the internet, whilst avoiding misuse and security lapses, is an increasingly difficult balancing act, says Florian Malecki – but there are solutions out there...

Schools need to have access to information for their staff and students, but there is a fine line between freedom of information and the risk of information abuse and loss. Educational establishments, like any place of work, need to protect their IT networks from viruses, malware, unauthorised access and data leaks, but at the same time, have a security system that is easy to use and affordable to manage.

The changing nature of the technology landscape, and the threats that accompany it, further complicate the situation. The number of web based applications that higher education users rely on and access from the school network continues to increase at a dramatic rate. This is due to the emergence of web 2.0 technologies, remote user access, and an increase in smartphone usage. School IT departments need to balance the use of productive applications versus non-productive and potentially damaging ones. In the case of Facebook for instance, there is a need for granular application control that supports policies allowing Facebook access for certain groups or individuals, but at the same time there is a requirement for disabling features that have no value, or that present opportunities for data leakage.

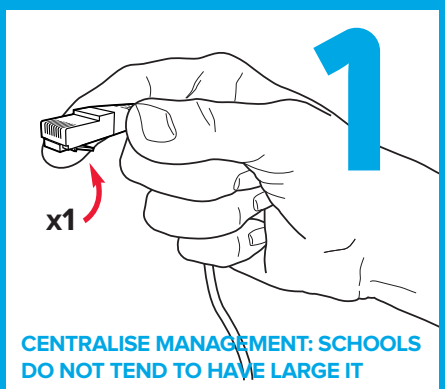
Cambridge Regional College recently addressed this as it updated its IT security to match its expansion. It now has a set of Dell SonicWALL solutions in place, which protect the school network but give teachers flexibility to make lessons current and engaging for learners. For example, they can allow students to have access to Facebook (while blocking Facebook Chat), and permit usage of YouTube and BBC iPlayer for research purposes. The lessons can be made fun and interactive for pupils, using the technology they are used to engaging with in their daily lives, but also allowing teachers and IT staff to ensure safe internet access.

Behind the wall

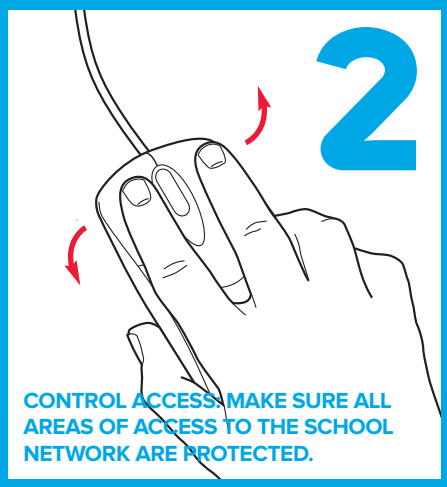
Major virus and worm outbreaks can be extremely disruptive, bringing down a school network, crippling day-to-day operations and requiring enormous clean-up efforts. To protect against threats, it is important for schools to stop breaches before they happen through a well-designed system of network access control and identity management. All devices attempting to log onto the network must be examined to verify that it complies with the necessary security policies e.g. has credible antivirus software installed, which is regularly updated.

Given the different levels of security required, schools need an intelligent, flexible system that can be managed centrally. One option is to install a Next Generation Firewall: a security product that includes multiple security features integrated onto one device such as network and application inspection, antivirus and network intrusion detection and prevention.

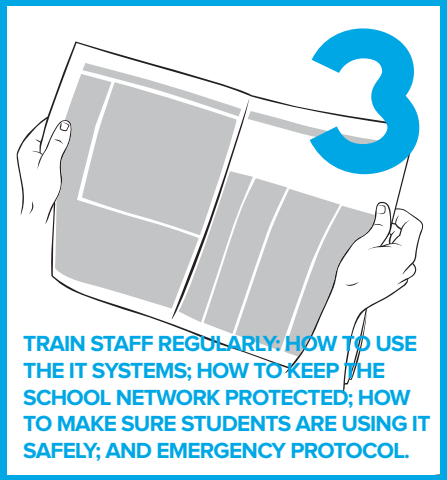
Through following the five policies outlined below, schools should be able to continue to deliver education in a fun and interactive way, whilst not bringing the system down through unwanted malware and viruses; a balancing act that is of benefit to everyone involved.



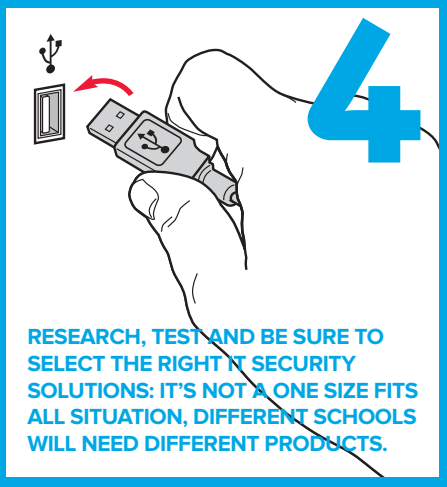
CENTRALISE MANAGEMENT: SCHOOLS DO NOT TEND TO HAVE LARGE IT DEPARTMENTS, SO THE SYSTEM NEEDS TO BE EASY TO MANAGE AND EASY TO FIX IF ISSUES ARISE.



CONTROL ACCESS: MAKE SURE ALL AREAS OF ACCESS TO THE SCHOOL NETWORK ARE PROTECTED.



TRAIN STAFF REGULARLY: HOW TO USE THE IT SYSTEMS; HOW TO KEEP THE SCHOOL NETWORK PROTECTED; HOW TO MAKE SURE STUDENTS ARE USING IT SAFELY; AND EMERGENCY PROTOCOL.

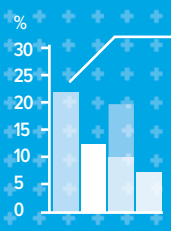


RESEARCH, TEST AND BE SURE TO SELECT THE RIGHT IT SECURITY SOLUTIONS: IT'S NOT A ONE SIZE FITS ALL SITUATION, DIFFERENT SCHOOLS WILL NEED DIFFERENT PRODUCTS.

SAFETY IN NUMBERS

26% OF 9-16 YEAR OLD SNS USERS HAVE THEIR PROFILE PUBLIC*

14% OF 9-16 YEAR OLDS HAVE SEEN SEXUAL IMAGES ON WEBSITES*



21% OF 11-16 YEAR OLDS HAVE SEEN POTENTIALLY HARMFUL USER-GENERATED CONTENT SUCH AS: HATE SITES (12%), PRO-ANOREXIA SITES (10%, RISING TO 19% OF 14-16 YEAR OLD GIRLS) AND SELF-HARM SITES (7%)*

*source: saferinternet.org.uk

KEEP UP TO DATE WITH TECHNOLOGICAL ADVANCES AS MUCH AS POSSIBLE, AS SECURITY THREATS WILL DEVELOP ALONGSIDE THEM.