

Oakbank School



FORENSIC SOFTWARE LIMITED SPECIALISES IN DEVELOPING, SELLING AND SUPPORTING DETECTION AND PROTECTION e-SAFETY SOFTWARE TO ENSURE THE APPROPRIATE USE OF IT RESOURCES BY EDUCATION ESTABLISHMENTS.

Stick or carrot? Inducement or enforcement? It's a conundrum probably as old as education itself but one which has been given a keener focus by the escalation of e-learning and the corresponding rise of network violations in schools and colleges.

Given the almost daily reported occurrences of computer and internet abuse, one would have hoped that students –especially those in the secondary sector – would have realised the need for self-restraint in their e-activities. This, unfortunately, is frequently not always the case.

What to do? Well, if you're an experienced school ICT manager like Mike Hanscomb, you'll have realised that, while the majority of students are capable of behaving sensibly on a school's computer network, there will always be a minority who do not respond to concepts such as 'social responsibility' and 'acceptable use'.

For these students, the most powerful deterrent to misconduct is the certain knowledge that they will be held to account for any misdeeds, and that any breach of acceptable behaviour can

and will be identified and recorded for disciplinary use. A cyberstick, if you will.

The cyberstick in question is Policy Central Enterprise (PCE), a powerful and innovative software program that has been in use at Oakbank School in Keighley, West Yorkshire for the past two years. Originally recommended to Mike and his colleague Kevin Allack by a fellow ICT professional, PCE has proved to be a huge success and has, he estimates, "reduced abuse of the school's network facilities to a tenth of what it used to be."

Here, for the technically minded, is how the network is set up. There are 530 XP Pro workstations in the school, 80 of which are used for administration purposes, and a further 80 laptops. The sixth form web site, the school's internet site and the VLE (Virtual Learning Environment) are run on Linux servers. Desktop machines in the computer suites run academic software such as Microsoft Office and Macromedia's DreamWeaver Suite. PCE runs on one of the school's 20 servers.

Students (the school's roll now exceeds 1800) have their own email boxes but email privileges are presently withdrawn from all Year 7 and 8 and



some Year 9 students because of misbehaviour identified by PCE. Students can connect to the internet on classroom desktop PCs or those in the Computer Suites but they are only allowed to transfer information on and off the network by using USB sticks or emailing digital data to themselves. Internet access” says Mike “is filtered by a local Network-Box firewall which amongst its many features incorporates filtering technologies such as Surf Control for web site access, email and http scanning. Its integration with our systems means that we have the ability to control internet access from full unrestricted access to no access at all for selected people using active directory security groups.”

An extremely robust system, one would think, which provides what Mike describes as, “a very secure and controlled environment” and a strong defence against would-be violators. Why would one need the further protection of a program such as Policy Central?

The answer goes to the heart of an ongoing education debate, which is: should a school lock down its network to such an extent that responsible students who genuinely want to research and retrieve information are denied that opportunity by the unacceptable activities of a minority? Mike thinks not, though he acknowledges that, “allowing adequate access to resources required by students carries a risk.”

The defining moment at Oakbank came with the realisation that “the email system was distracting pupils badly during lessons and, quite frankly, was being used as an informal instant-messaging / chat-room facility. We wanted to address that and still allow as many pupils as possible to continue to use e-mail.”

This, he points out, is where Policy Central is so important. “We can pick up those students who choose not to follow the Acceptable Use Policy and take the appropriate action. We basically achieve this by picking up on defined keywords in

the customisable Policy Central Library which then presents us with the hard facts. It will pick up any abuse of the school’s network and report it back to us. Without Policy Central we would never know the true picture and in what areas we need to improve our security and control.”

Three colleagues work with Mike in the ICT Support Department, one of whom spends an hour a day sifting through the Policy Central logs and forwarding the relevant information to the ICT Teaching Department. They then decide what internet/email sanctions should be applied and the school sends letters - with screenshots of the offence - home to parents.

More, ‘Lord of the Flies’ than ‘rose tinted’ in outlook, Mike, in common with the most ICT professionals working in education has a pragmatic, unsentimental view of students’ e-activities and their capacity for misbehaviour. It’s a view that’s based on first hand observation. The most frequent misuse of the Oakbank network is abuse of the email system, but PCE has also picked up on and reported on many other types of inappropriate activity.

The school has a comprehensive Acceptable Use Policy (AUP) drawn up jointly by the ICT Support Department, the ICT Teaching Department and the Deputy Head, who has the ultimate say in any disciplinary matters at Oakbank. Students sign an AUP at the beginning of year 7 and thereafter “click an onscreen ‘OK’ button to acknowledge the AUP each time they log on.” This, Mike believes, “has zero effect and is in no way a deterrent. It seems that many pupils do not take responsibility for themselves unless they know that the system will pick up their misdemeanours and consequences will follow from that.”

This, ultimately, he says, is the value of PCE to us. No other program we have come across can give us such a complete picture. There are lots of other proactive security products on the market but they may well have

flaws we would never know about. PCE doesn’t age like these tools and, in my opinion, facilitates the far more effective strategy of letting users know that they will always be caught.”

Increased broadband availability has meant that unwelcome and unsavoury practices have become far more widespread. The need for e-security, Mike points out, has become paramount and the only sure way of knowing how well your security system is operating is for a product like PCE to be actively monitoring and recording abuse of the network.

“We depend” he says, “on this program heavily, and as an ICT professional I genuinely feel reassured that PCE is protecting us all.”

Recommendations don’t come better than that.

“ We can pick up those students who choose not to follow the Acceptable Use Policy and take the appropriate action ”

Mike Hanscomb

ICT Manager

Oakbank School