



Non-Restrictive Technology in Education

The reboot-to-restore concept

June 2009

Written in association with:

ICT Networks Ltd

8 Palmerston Street

Stoke on Trent

Staffordshire, ST1 3EU

Email: sales@ict-networks.co.uk

Tel: +44 (0) 1782 406406

Fax: +44 (0) 1782 406444

Introduction

Computer literacy is now a highly-desired skill to learn in schools, and under new recommendations, a core skill for English Primary School children. Educational institutions, where more and more people are learning their computer skills, represent a unique and complex learning environment from a technological standpoint. Educational computer networks must provide the appropriate equipment to instruct students in technological learning that meets the highest requirements, and they must provide state-of-the-art equipment that is consistently operable and available. This is growing increasingly difficult to achieve because of the volume of users in educational networks, the variety of hardware, the multi-faceted threats facing the educational technology industry, and the ever-growing requirements for what the industry must achieve. This problem has been exacerbated by the introduction of large quantities of netbooks and laptops into the school environment.

Educational instructors are faced with the conundrum of providing students with access to technology so that students are appropriately educated; yet they are having to continually tighten security because of the growing number of threats present both internally and externally. This white paper discusses some of the technological issues facing education, outlines the typical and traditional responses to these issues, and describes an alternative approach in the form of non-restrictive technology and the reboot-to-restore concept.

Educational Environment Computing Situation

Learning computer skills is a necessity for today's students, but there are several problems that educational institutions must deal with in their day-to-day management of computer networks.

Security Threats

Malware—in the form of spyware, viruses, rootkits, Trojans, and keyloggers—have become a pervasive and increasingly unmanageable problem. IT staff often have a suite of products to combat the different forms of malware, such as anti-spyware, antivirus, and adware programs that are installed and run frequently on lab machines. These products require management and maintenance; IT staff spend time ensuring that definition files are updated and that patches are applied when they are released.

The high volume of multiple users on the lab machines in an educational environment results in users accessing websites or using removable media that could potentially invite malware into a system. The constant management of malware can result in IT administrators locking down certain sites and programs that have been deemed problematic. While this can mean a decrease in malware, it can also mean that the learning environment becomes more restricted for students.

Malicious Users and Innocent Clickers

Students are growing more computer savvy every day, and can be more knowledgeable than their instructors in certain areas. They are capable of downloading programs that can damage a computer—file sharing and peer-to-peer programs, keyloggers, and several other programs that can take up bandwidth and affect the efficiency of the lab and of the system. Conversely, “innocent clickers” who are unaware of the consequences of their actions can cause serious damage to an operating system.

Between these two types of users, IT administrators are continually fighting computer configuration drift—that is, the drifting of computer configurations and settings away from their baseline and optimized state. This makes things difficult for instructors who need a uniform environment to teach their classes, as the amount of time and

resources used to manage this problem can be staggering and financially draining.

Government Economic Support

The United Kingdom government has been running an extensive ten year programme of investing in educational information technology, starting with NGFL and progressing through mass procurement of interactive white boards, caching servers, and the roll out of BSF. More recently, the Department of Children Schools and Families launched “Computers for Pupils,” a two year, £90 million pound programme aimed at helping disadvantaged secondary school children improve their education and life skills by placing a computer in their home.

Many schools have procured laptops or netbooks for distribution among eligible pupils. Schools have often supplemented central government funding with money from their own budgets and purchased additional hardware to ensure that an entire year's class is issued a mobile computer. Keeping these computers in a usable condition when they are removed from the protected environment of the school and its network can be an onerous task.

In April 2009, Sir Jim Rose published his review of primary education commissioned by the UK Government. In the report Sir Jim places IT as a core skill alongside numeracy and literacy. It states, “Children use and apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts. They become independent and discerning users of technology, recognizing opportunities and risks and using strategies to stay safe.”¹

Interestingly, the document recognizes that children need to develop strategies to stay safe—the implication being that children should be exposed to some elements of risk. Traditional locked down networks fail to give the user a “real world” IT experience.

IT Resources

In education, a typical ratio of IT support staff to computers is 1:500. Not surprisingly, IT staff are frequently stretched to the limit, and often spend the majority of their time re-imaging and rebuilding machines to keep them up and running. The rebuilding or re-imaging can happen on a weekly or even daily basis, leaving little or no time to make other improvements to networks, or work on troubleshooting other issues. This can result in technological demand outpacing technological support, and helpdesk calls escalating beyond control.

As a result, IT staff prefer to lock down machines to prevent users from damaging the machines so they don't have to spend all their time rebuilding them. This means the IT staff have more control over classroom policy than teachers do, because the IT staff don't want or don't have time to be constantly rebuilding workstations. This begs the question—where will the next generation of programmers, IT staff, and computer scientists come from if current students are all locked out of various functions?

Approaches to Security

Lock Down Approach

The most common response to the technological issues facing education has been restrictive. IT staff lock down computers to prevent any mischief by students, or as a defence against malware. This response means less rebuilding of machines, but can place severe restrictions on the part of the students' learning environment. This

¹ <http://www.dcsf.gov.uk/primarycurriculumreview/downloads/EssentialsforLearningandLife.pdf>



can be difficult to implement on a machine that is used both at home and in the school.

Reactionary Approach

If networks are not locked down, the IT staff are most likely using a reactionary approach to maintain security. The reactionary approach means dealing with computers on an individual basis and using re-imaging or rebuilding as a method of keeping computers uniform and protected. However, the problems with this approach are many, given the amount of time it takes for the rebuilding process, and the correlating downtime of the machine. This approach is also only a temporary one, and does not deal with the cause of the problems faced by the networks.

The Non-Restrictive Reboot-to-Restore Concept

What if there was a better way? What if IT staff could be assured of not having to re-build damaged workstations but students could still have unrestricted access to computers and be allowed to do whatever they want?

The non-restrictive, reboot-to-restore concept makes this possible. This approach allows students to learn in an unrestricted environment without damage to the computer. Students can freely learn about operating systems and experiment with different programs. They can customize their desktops, delete or create shortcuts, and do virtually anything they want to the computer; the computer's original configuration is always restored upon reboot. Teachers are assured of a uniform environment in which to instruct; students are guaranteed an unrestricted, available, and perfectly functioning machine; and IT staff does not need to spend valuable time rebuilding or re-imaging machines.

Non-Restrictive Technology Benefits

The benefits of non-restrictive technology are many:

- offers an unrestricted learning environment for students with improved efficiency levels
- eliminates obstacles to integrating technology in learning
- gives students the freedom to experiment and learn without penalty or consequence
- enhances system performance due to improved resource utilization efficiencies
- enhances computer performance by eliminating the need for most routine hard drive maintenance
- ensures consistent configurations
- reduces unnecessary anxiety related to allowing users access
- improves the classroom technology experience
- allows user full access to computer without time-consuming management restrictions
- significantly lowers Total Cost of Ownership for technology assets because of a vast reduction in time and cost spent maintaining and rebuilding machines
- eliminates the hidden costs present in the time teachers spend troubleshooting computer issues

Non-Restrictive Technology Solution: Faronics Deep Freeze

Faronics has been a pioneer of reboot-to-restore technology since 1999. Faronics Deep Freeze offers a non-restricted learning environment for students, uniform labs for teachers, and leaves IT staff free for more valuable and proactive activities. Once Deep Freeze is installed on a workstation, any changes made to the computer—regardless of whether they are accidental or malicious—are never permanent. Deep Freeze provides immediate



immunity from many of the problems that plague computers today—inevitable configuration drift, accidental system misconfiguration, malicious software activity, and incidental system degradation.

Deep Freeze ensures computers are absolutely bulletproof, even when users have full access to system software and settings. Users get to enjoy a pristine and unrestricted computing experience, while IT personnel are freed from tedious helpdesk requests, constant system maintenance, and continuous configuration drift. Retaining user data across restarts is easy, if so desired. By mapping user and application data to a Thawed (unprotected) partition or drive, users are able to store their documents, pictures, music, etc., while still enjoying the total system consistency that Deep Freeze offers.

Deep Freeze also offers flexible options that enable IT administrators to easily create automated update and maintenance periods. Deep Freeze maintenance periods can be scheduled to allow system and virus definition updates to occur at predefined times—either with the Deep Freeze Enterprise Console or using your preferred third-party desktop management solution.

The benefits offered by Deep Freeze are many:

- offers the ability to standardize workstation configuration, from the programs installed to the placement of icons on the desktop
- allows for permanent, scheduled, or ad hoc updates to the operating system and software
- downtime is reduced dramatically, in correlation with a vast reduction in maintenance costs
- computers no longer have to be rebuilt or re-imaged; eliminates all software-related issues
- computers are returned to their original configuration with a quick reboot
- has a small footprint; little disk space is required
- integrates seamlessly with all third-party management applications
- can be easily controlled and configured via the GUI Enterprise Console
- requires no maintenance; no definition files to update and no patches are needed

Conclusion

A better way exists that enables users to have unrestricted access to computers so that they may do whatever they wish. IT's workload will not increase as a result, because the non-restrictive, reboot-to-restore concept keeps computers running in their optimal configuration. By using Deep Freeze by Faronics, teachers are assured of a uniform environment in which to instruct; students are guaranteed an unrestricted, available, and perfectly functioning machine; and IT staff do not need to spend valuable time rebuilding or re-imaging machines.



Contact Us

Web: www.faronics.com
Email: sales@faronics.com
Phone: 800-943-6422 or 604-637-3333
Fax: 800-943-6488 or 604-637-8188
Hours: 7:00am to 5:00pm (Pacific Time)

Address: Faronics Technologies USA Inc.
Suite 170 – 2411 Old Crow Canyon Road
San Ramon, CA 94583
USA

Faronics Corporation
620 - 609 Granville St.
Vancouver, BC V7Y 1G5
Canada

About Faronics

Faronics' solutions help organizations increase the productivity of existing IT investments and lower IT operating costs. In today's economic climate of increasingly tightened budgets, continuous market pressure, and more work to do than time available, this is critical. With a well-established record of helping organizations manage, simplify, and secure their IT infrastructure, Faronics makes it possible to do more with less by maximizing the value of existing technology.

This is what we do.

Incorporated in 1996, Faronics has an office in the USA and Canada, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 customers.

Copyright

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your/an organization, and thereafter it may not be re-copied, reproduced, or otherwise distributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.