

Blue Reef Biz Talk

Laptop programs – defining risks and responsibilities and implementing safeguards

As a School Principal am I responsible for what students do with a school-provided laptop at home?

Extension of “Duty of Care” beyond the school boundaries

Today the internet is an integral part of every student’s educational tool box with schools providing access across the student age spectrum. In the past internet services were limited to school labs and libraries and were operated in a controlled environment. With the ongoing adoption of 1-on-1 laptop programs, schools are now facing a situation whereby more than 60% of all devices will be mobile and will move with the student to alternative locations such as home, boarding houses, etc.

Two serious questions need to be answered by the school community:

- Are we responsible for what students do with a school-owned device outside of school boundaries?

and

- If the mobile device is not school equipment, are we still responsible?

Challenges

The challenges schools face can be divided into three groups: Governance, Policy Management, and Enforcement Technology and schools need to ask the following questions:

Governance:

1. Do we have a well-defined policy of appropriate usage for school-owned laptops both inside and outside school?
2. Do we have a well-defined policy for the use of private and unregulated laptops?
3. Do we have a well-defined School Internet Services document that sets the appropriate service level expectations from mobile users?
4. Have we defined the administration and IT processes necessary to manage and support mobile devices, FAQ, and help desk?
5. Have we involved parents and custodians sufficiently for them to fully understand the benefits and responsibilities inherent in the school’s 1-on-1 mobile program plans and sign off on them?

Policy Management:

1. Content Control: Does the same school usage policy apply at home? Or is it a looser basic policy?
2. Logging and Monitoring: Where and when do we track information and how do we report on it?
3. Laptop security: Does the school allow the student to control installation and removal of software on a school-provided laptop?
4. Software image: How does the school keep the laptop up-to-date with all security and software updates?
5. Endpoint: when is a mobile device considered “compromised” (hacked or infected) and in need of a thorough clean-up before being allowed back on the network?
6. Connectivity: What is our policy when the mobile device is away from the school?

Technology Enforcement:

1. How do we inspect content on mobile laptops?
2. Do we force all traffic through the school internet connection?
3. Do we use an external policy server outside of school? And if yes, do we need to manage two separate content policies?
4. How do we prevent students from removing our controls from the mobile devices?
5. How do we record student activities when they are at home?
6. How does the mobile device know when it is in the school network, and when it is at a remote location?
7. How do we identify a school user and apply the appropriate policy when the student is at home?
8. How do we provide parents and custodians with the ability to view the student's activity on this mobile device?

Blue Reef Solution

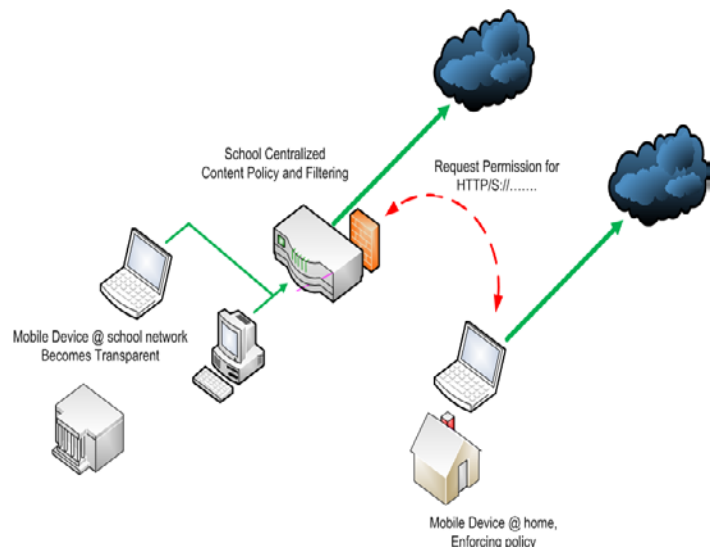
Mobility has always been a challenge for educational institutions. It is a risk management exercise which must take into account each organisation's unique situation and will inevitably involve a balancing act between constraints and compromises.

If a school adopts the following policy decisions...

1. Mobile devices will be locked by the school and students cannot remove controls.
2. All traffic will go through the school internet connection while the devices are at school and home user's data won't traverse through the school network while the devices are at home.
3. Mobile devices will have a basic content policy which will apply to all users at home.
4. Reporting and monitoring will be done per mobile device.
5. Mobile device images will be centrally managed by IT.

...then the following can best practice solution can be implemented:

1. A school network content control can be implemented for all static and mobile devices.
2. Enforcement technology can be implemented on the mobile devices.
3. Mobile control on each device will ask permission from the school's policy decision point and then allow or prevent access to the requested web site.
4. When the mobile device is on the school network it will be subject to the school's main policy control and will be transparent.
5. When the mobile device is used off-site (away from the school network), a default policy can be applied to unknown users (for instance the student's parents), and a customised policy for known users.
6. If a mobile device has been identified as compromised then its request will be redirected to a block page which informs the user there is something wrong with the machine.



Blue Reef Best Practice

Blue Reef is the first choice Internet Management Provider to over 300 educational institutions throughout Australia. We have been assisting schools achieve solutions to enable successful 1-on-1 laptop programs for over a decade. Our extensive experience in the development of tools, policies and technology to address these types of education needs is unsurpassed.

Blue Reef's holistic approach to providing a solution for 1-on-1 laptop programs and extension of Duty of Care outside of school is based on our understanding, capabilities and experience with combining multiple technologies to achieve maximum efficiency.

The Blue Reef Solution for extending Duty of Care to the home offers the following benefits:

1. A template for Acceptable Usage Policy (AUP) for mobile devices
2. Sonar Internet Management Platform to address School and Remote Content controls which includes:
 - a. Centralised transparent network content filtering with user-based policies
 - b. Compatible with Microsoft Windows, Apple Macintosh, and Linux platforms
 - c. While off campus, mobile computers still communicate to Sonar at the school to get authorisation for content
 - d. Mobile device transparency when on school local area network
 - e. Full logging and monitoring of per user activity regardless of location
 - f. Per user reporting showing which websites students have visited and logging any suspicious or inappropriate activity

Blue Reef's Best-of-Breed and Quality policy:

Blue Reef's 10 years experience in solving educational challenges in different customer environments has always been based on adopting high quality, best-of-breed and third party technologies with proven track records.

Consequently Blue Reef has close partnerships with the leading suppliers of Content Categorisation such as Secure Computing, and with leading Anti Spam engines such as CommTouch.

Blue Reef has recently partnered with NetSweeper best-of-breed client interception technologies. NetSweeper is an international US-based vendor, which has specialised for more than 10 years in providing interception solutions for mobile devices.

Blue Reef will be using NetSweeper mobile interception technology to communicate to our Sonar Appliance to enforce content policies on mobile devices

About the Author

Guy Lupo, VP Products & Services, Blue Reef Pty. Ltd. has 20 years experience in governance, compliance and security in the enterprise and education spaces, and is continuously working with educational organisations to improve their processes and supporting technologies to achieve better educational outcomes.

Guy's career history includes strategic product and management roles with worldwide international leaders such as Check Point, CA, Microsoft, Cisco, BMC Software and other start-ups in the Governance, Compliance and Security space.