Enabling BYOD in K-12 with Seamless Mobile Device Accountability and Control
How to ideally support mobile devices and maintain Web security and policy compliance in your schools

Introduction
The proliferation of Smartphones and other Web-enabled mobile devices has dramatically altered the way schools utilize online learning resources. Users are no longer physically tethered to workstations in fixed locations. Today, students and staff can utilize multiple types of devices and computers to connect to the Web in a wireless network environment. Many schools want to enable this kind of device flexibility, commonly known as Bring Your Own Device, or BYOD, but are hesitant to deploy it due to security and compliance concerns.

BYOD is fraught with a multitude of serious IT risks, potential costs, CIPA compliance loopholes and child safety issues. There is a clear need to approach the security concerns around BYOD with a degree of caution and informed advice.

What is required is a simple and secure solution for BYOD scenarios in education environments that is cost effective, flexible, proven, reliable and (perhaps most importantly) easy to support and implement.

Mobile Device Accountability and Control
At ContentKeeper we call this solution concept Mobile Device Accountability and Control (MDAC). This is merely a way of defining the security capabilities that K-12 organizations are looking for to answer the risky questions around BYOD adoption. For ContentKeeper, MDAC is a built-in capability in our standard Web Filtering technology solution.

Enabling BYOD means that schools can embrace next-generation learning with next-generation technology, and do this affordably, without additional IT resources or effort. It also means that schools can enable students and staff to work how they want to work, without compromising security, compliance or student safety.

What is Driving BYOD Adoption?
BYOD is a rapidly growing concept driven by the exponential growth of Web-capable mobile devices and Smartphones. This coupled with widespread and readily available wireless Internet access has meant that students and staff are bringing their own mobile computing devices onto the school network. Schools want to be able to monitor these devices on their network and students and staff want to be able to utilize their own devices at school, which are normally prohibited.

A 2013 survey on Bring Your Own Device (BYOD) uptake by Holger Schulze that polled 160,000 IT professionals found the biggest positive benefits of adopting BYOD included:
- Greater user satisfaction by enabling users to utilize their preferred mobile device.
- Improved mobility and flexibility enabling users to access the Web when and where they need to.
- Improved productivity of online resources as a result of greater flexibility and enabling users to work on devices that they are most familiar with.

However, BYOD introduces many challenges to maintaining IT security, CIPA compliance and safeguarding student data and privacy. The same Holger Schulze survey found that the biggest concerns with BYOD were:
• Ensuring authorized Web/network access and (for example) maintaining CIPA policy compliance
• Preventing data loss
• Increased exposure to malware attacks

Schools are looking to enable BYOD because of the aforementioned benefits. But, many are hesitant to do so or unsure how to approach it with limited budgets, resources and already established Web filtering technologies which don’t natively support BYOD requirements.

This Whitepaper examines how schools can support BYOD and mobile device 1:1 deployments with ContentKeeper technology while mitigating and even eliminating many of the common pitfalls. We will look at how BYOD is driving major changes in K-12 IT requirements and how education organizations can achieve the level of Mobile Device Accountability and Control (MDAC) they desire with a minimum of effort, cost or disruption to their existing IT infrastructure.

What is BYOD?

BYOD essentially refers to the ability for a student, staff member or guest to bring his or her own mobile device on campus and connect to your school network. They can access the Internet or if allowed, other internal network resources while being CIPA/policy compliant even though on their personal device.

In a K-12 environment BYOD is mainly student focused to enable anytime/anywhere learning, but administrators and teachers should also be considered when deploying BYOD. Students are trying to bring their devices to school so BYOD is becoming a technology requirement for next-gen learners. Regardless of where your school is in this evolution, BYOD is a reality today because of budget constraints schools and districts face and not being able to refresh 1:1 initiatives so IT is trying to take advantage of student devices and make BYOD a reality.

A proper BYOD strategy allows the use of any device, enables the school to identify the user, enforces the right policies and reports on the user’s activities, without necessarily requiring a client to be installed on the device or requiring major IT configuration changes.

What Devices are Supported?

ContentKeeper supports any type of device running any operating system. This includes:

- Laptops and notebooks (Apple, Android, Chrome or Windows)
- iPads and other tablet devices
- Smartphones, iPhones and other Web-capable mobile devices using TCP/IP and Web Protocols

Because ContentKeeper is an in-line solution (a Layer 2 Ethernet bridge design) the application of filtering and deep packet inspection is both device and O/S (Operating System) agnostic. Put simply, this means that MDAC can be applied to any Web traffic, to or from the Internet, regardless of the device used. Additionally, due to this design Web Filtering is faster and more scalable than traditional proxy-based filtering technologies which process Web traffic at the application layer (layer 7).

User Authentication and Directory Integration

ContentKeeper customers are able to effectively support a proper BYOD strategy within their existing environment by using the “Form-Based Authentication” method of user resolution. This enables your school to support any number of devices without the need for client software installation or previously registering the device.

To the user a proper BYOD strategy means simply connecting whatever mobile device
students have to the school’s wireless network. When a student or staff member first tries to browse the Internet, an authentication page appears as displayed below. Users can either authenticate to get their normal web browsing policies enforced on that device, or if they are a guest user they can ignore this authentication request and be treated as an unauthenticated user. In this scenario the default browsing policy or restrictions can be whatever you wish to set for this purpose. The screenshot below shows the authentication page as seen on an Apple device, it can be fully customized:

The “New BYOD / Desktop Registration” screen, as shown on the top of the next page, shows a generic device registration browser prompt that can be displayed on any device. This process requires no software installation and ensures a user must register a new BYOD mobile device they bring to school. This system allows users to bring their own devices on campus, but requires network access authentication which in turn provides activity reporting for all devices users browse the Web from. This consistent tracking of authenticated Web use across multiple devices is essential to maintaining accurate reporting and effective CIPA policy compliance.

A network administrator can create any number of groups of related account types for students and staff. This means that when a user registers their device they can be granted filtered Web access based on the privileges granted to their account type. Users can be authenticated using a variety of methods:

- Guest Account – this can be used for unknown users or visitors and enables access to a limited set of Websites such as Intranet and approved websites.
- Directory Authentication – ContentKeeper integrates with many common User Directory services such as Active Directory, eDirectory, OpenDirectory, Radius and LDAP. Authenticated users can then browse the Web from their device according to their account privileges.
- Federated Authentication – Supports authentication with Google directory services.
- Open Registration – Requires the user to provide information about themselves and
links the user with the device MAC address.

- Secure Registration – Requires the user to register an email address or phone number and dynamically generate an access password.

With this process, the user is normally authenticated as long as the Web browsing session remains open. Flexible options within ContentKeeper enable you to set time-out periods, requiring re-authentication once a session is inactive for a set time. Or, if you prefer, ContentKeeper can be configured to “remember” the device and every time that recognized device is seen on the network it can be linked to the registered user account automatically.

1:1 Device Agent (Optional)
For 1:1 deployments ContentKeeper provides a lightweight 1:1 device agent which can be installed on devices and easily rolled out using a variety of methods (such as Group Policy). The agent is similar in some respects to a browser Cookie and automatically authenticates the device without the need to manually log in.

With certain types of devices, such as Apple devices, the agent produces a “heartbeat” which regularly updates ContentKeeper with information about the device and the session. This in turn enables detailed real-time reporting of active devices and browsing sessions on the network, as it happens. This enables IT administrators to constantly monitor what devices are on the network and block or manage new devices as required.

Another key advantage of the optional lightweight device agent is that it can report on the configuration of the device and alert administrators to the presence of devices running unauthorized settings, applications or fixed device configurations that have been tampered with (profile tampering detection) or “jailbroken”. This gives IT administrators the power to block certain types of devices or device configurations from the network if desired or report on devices running unwanted software that may pose a security risk.

Mobile Device Accountability and Control

Once a device is registered on the network and the user is authenticated as either a known or guest account, ContentKeeper continually tracks Web use generated on that device. School IT administrators can see, at a glance, what devices are being used on the network, by whom and what for.
This screenshot above shows the ContentKeeper administration view of devices as they appear on the network. The administrator can see:

- What type of device is being used and the manufacturer
- What software version of the operating system is installed
- Which user is browsing on the device and how the user was authenticated
- How long the user has been browsing the web in the current session
- The device IP address and MAC address

In 1:1 device management scenarios (where the device is allocated to the user by the school) the agent can ensure that the browsing activity on the device is adhered to even when the user is off the network such as using public Wi-Fi, 3G/4G networks or using the device from home.

In Conclusion

ContentKeeper ensures that BYOD can be seamlessly supported with centralized device management and no requirement of special software or costly disruption to your current IT infrastructure. ContentKeeper’s special in-line Layer 2 Ethernet Bridge design allows you to deploy BYOD quickly and easily and works with any existing school network infrastructure or can be hosted in the cloud if desired.

ContentKeeper also supports large scale state and regional education networks that maintain systems for multiple districts. This means that in environments where a single IT provider may be responsible for multiple schools with different policy requirements, ContentKeeper can still enable seamless Mobile Device Accountability and Control for all of those schools and different devices without additional costs or special hardware.

Disclaimer: The information herein is provided for informative purposes only and is offered “as is” without guarantee, either express or implied, including but not limited to the implied warranties of merchantability, fitness or a particular purpose, and non-infringement. ContentKeeper Technologies is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publically available sources. Although reasonable effort has been made to ensure the accuracy of the data provided, ContentKeeper Technologies makes no claim, promise or guarantee about the completeness, accuracy, timeliness, or adequacy of the information and is not responsible for misprints, out-of-date information or errors. ContentKeeper Technologies has no warranty, expresses or implied, and assumes no legal responsibility for the accuracy or completeness of any information contained in this document.