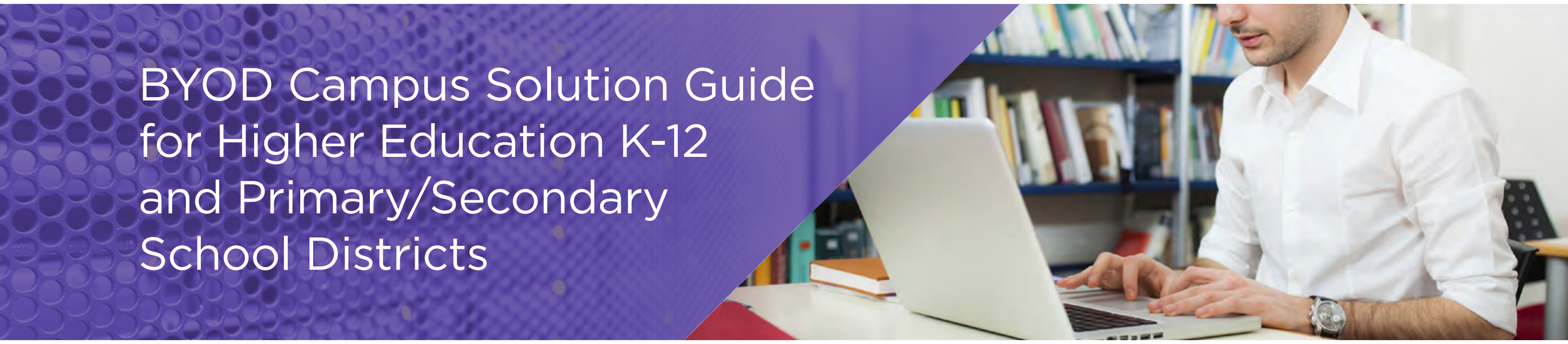
BYOD Campus Solution Guide for Higher Education K-12 and Primary/Secondary School Districts



Educational technology is enabling colleges and primary/secondary school districts to reshape how students are taught. Mobile student devices have ushered in a new era of personalized learning with digital content delivery, flipped classrooms, eTextbooks, adaptive learning, and the concept of competency-based education. These new styles of learning in turn require that every student have access to a computing device on the school network. Many students now own personal Wi-Fi devices that may also be permitted to connect to the network in certain locations and during specified hours. To address these needs, colleges and primary/secondary school districts are implementing Bring Your Own Device (BYOD) on their campuses. Here are the critical technology issues facing colleges and school districts as they implement the BYOD computing. Addressing these issues brings colleges and school districts another step closer to achieving the objectives of learning success for all students.

Critical Technology Issues for Campus BYOD

DELIVERING HIGH SPEED DIGITAL CONTENT

First and foremost, all BYOD programs require pervasive Wi-Fi coverage across the campus both indoors and outside. The network must be capable of connecting to all Wi-Fi devices that students and faculty are likely to bring on campus. The digital content to and from the BYOD devices will vary from text to high definition video, and the network bandwidth will need to fully accommodate that range. To operate smoothly, there can be no bottlenecks from the Wi-Fi access points, back through the wired switches, and all the way to the broadband Internet connection and the data center. These connections must be highly available or fault tolerant to insure uninterrupted teaching.

PROTECTING STUDENT SAFETY AND PRIVACY

While the network must be capable of connecting all devices, it must also be very selective in doing so. Authorized devices should be expeditiously and effortlessly onboarded, while unauthorized devices must be prevented from gaining access to the network. The best way to implement this is with a defined policy as to which devices, users, and apps can access the network resources from defined locations at specified times of day. This policy needs to be implemented consistently across the network. Firewalls prevent access from outside sources and web filters prevent visits to malicious sites that can damage the network. Network integration with firewalls and web filters means that policy can be smoothly implemented across all resources. The network must be capable of both controlling and monitoring all devices and network activity.

MONITORING NETWORK ACTIVITIES

A constant risk to network, IT resources, and campus in general are unapproved applications and rogue devices that may appear on the network and either permit unauthorized access or interfere with other devices. A means to monitor all devices and applications that operate across the network is vital.

GUEST ACCESS

In addition to easy onboarding of district-owned devices, a simple method for onboarding guest devices and instilling them with the appropriate access to Internet resources must be provided.

APPLICATION INSIGHT

Visibility into application usage, website access, bandwidth consumption, and patterns of activity are important for optimizing the user experience and verifying that digital educational content is adequately delivered. This is also vital for optimizing the infrastructure and for both short- and long-term planning.

COMPREHENSIVE SERVICE AND SUPPORT

Access to a global technical access center (GTAC) on a 24x7 basis ensures that all support questions can be answered promptly to keep the network functioning at all times. Prior to installation, it is important to survey and assess the RF characteristics of the site to determine optimal placement of access points and switches. Depending on the network support resources available within the district, network training and managed services may be required.

Extreme is the only company in the industry that takes an architectural approach to bringing products to market from R&D to product release. As a result, all of our network products from wireless to wired are managed by a single NetSight network management console for easy administration by resource-constrained IT teams. Our open, standards-based, and comprehensive SDN enables simple integration with third party technology such as web filters and firewalls. Extreme Networks has over 1,400 district customers spanning more than 17,000 schools nationwide, delivering the best educationally-focused networking solutions in the industry.

To learn more see our solution guides for Online Testing and Digital Citizenship, Student Privacy and Safety and visit Extreme Networks K-12: Primary / Secondary Education Solution Center.

RESOURCES

London District Catholic Schools Case Study
Bringing Order to the Chaos: A BYOD White Paper

EDUCATION SOLUTION GUIDES

One-to-One Computing
Online Testing
Student Privacy and Safety

REQUIRED CAPABILITIES	RECOMMENDED SOLUTION	HOW WE DO IT BETTER
High Density, Pervasive Wi-Fi Connectivity	• AP 3805 802.11ac Access Points (2x2:2) • AP licenses, Radar licenses • 2x V2110 virtualized controller for high availability (for up to 1050 APs)	• Highly scalable, seamless and secure mobile Wi-Fi connectivity
Wired Edge and Backhaul	• X460-G2	• High performance wired backhaul, cross-platform stacking, embedded application controls, PoE+
BYOD Onboarding and Network Access Control Monitoring of network and all devices Guest access	• NetSight® • Mobile IAM	• Consistent device policy based on over 40 attributes centrally implemented, enforced end-to-end • Simple device onboarding, 100% fidelity of all IP assets • Internet filter and firewall integration, MDM integration
Device and Application Usage Visibility and Insight	• Purview™ Analytics	• Visibility into applications and websites being accessed with reported user experience measurements from every part of the network
Services and Support	• Maintenance • Training • Professional Services	• Extreme Networks' Global Technical • Support Center (GTAC) provides technical support • 24 hours a day, 365 days a year; and our Networks SupportNet offerings let you choose the exact level of service ideal for your organization

Extreme® networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800