BYOD

Security Policy and Procedures Guide for Schools

securEdge networks

AUTHOR PAGE:

Philip Wegner

Philip Wegner is a technology entrepreneur, Founder and CEO of SecurEdge Networks. SecurEdge is an IT Solutions company that has helped hundreds of organizations plan, deploy and support technology that allows for the secure operation of wireless devices.

FOLLOW ME ON TWITTER @PHILIPWEGNER

TABLE OF CONTENTS:

Share this eBook!

securEdge networks
SecurEdgeNetworks.com

CHAPTER 1

WHY BYOD?

Before we jump right into the BYOD policy suggestions, lets make sure we are on the same page about why to choose BYOD for your school. Let's start with the basics.

What does BYOD mean for education?

As you probably already know, BYOD stands for Bring Your Own Device. A BYOD policy allows students to bring personal devices, such as e-readers, smartphones, netbooks, and tablets like iPads in the classroom for use as a learning tool. This popular trend started in the workplace, but has now spread to classrooms everywhere. A properly and effectively implemented BYOD solution can create an environment where students can remain plugged in and engage in using their own devices as 21st century learning tools.

What is Driving BYOD in Schools?

Education systems must adjust to better accommodate the way students learn today, and for today's students that includes the use of technology.

The confluence of the desire for increasing use of technology in schools and increasingly shrinking educational budgets is driving the move toward a BYOD environment in schools. Also, since many students already use the highly portable devices at home, teachers can easily incorporate their use into coursework. A BYOD policy can be viable plan for schools wanting to save money, while still providing students with the access to up-to-date technology.

84% **of schools who do not currently allow BYOD stated that they receive frequent requests from students and faculty to use their own devices on the network.**

What are the benefits of BYOD in Education?

Schools all over the United States are implementing BYOD solutions and reaping fabulous benefits. For schools, BYOD can encourage collaborative education, increase student engagement, and allow opportunities for more personalized learning where students can excel at their own pace.

Students' personal mobile devices tend to be more cutting-edge, so schools can more easily stay up-to-date with technology. BYOD is a way for schools to get closer to that 1 to 1 (every student has a device) model without incurring the higher costs of a 1 to 1 model.

What are the potential disadvantages of BYOD?

BYOD typically means more devices to support. They are relatively unmanaged and potential security risks. Personal devices could also be misused as a distraction rather than a learning tool.

Since the school doesn't own the device which means they have less control of the device type, image and security settings. The network has to be designed to control the behavior of the device and manage risks. If you haven't properly prepared your wireless network infrastructure these mobile devices can overload your wireless network.

Also, if you do not have a well-planned BYOD policy in place you could end up with your IT staff being constantly overwhelmed with questions and device support issues making BYOD a nightmare for your IT staff.

Why do I need to create a BYOD policy?

Creating a solid BYOD policy takes time and careful planning, but it is critical to successful BYOD implementation in schools. It is essential to make sure you are securing all those mobile devices and educating students, parents, and educators on policies, guidelines, and best practices.

Having a BYOD policy that covers all the right bases not only covers your rear, but also makes the whole BYOD implementation process much easier.

There is not a one-size-fits-all solution when it comes to building a BYOD policy. Each schools BYOD policy will vary based on the schools or school districts individual needs, but there some points that every educational facility should consider. The next chapter describes the top BYOD Policy considerations.

CHAPTER 2

11 BYOD POLICY CONSIDERATIONS

1 Describe the Overall Goals of Your BYOD Program

It's important you describe the reasons your school chose to implement a BYOD program as well as the specific goals of the BYOD program. Although your students may be excited, you will still probably have some leery parents and educators that need extra convincing. Stating all the benefits of the program, the reasons for implementing it, and goals upfront is a good way to start any BYOD policy.

2. State Which Devices You Will/Will Not Support

You need to choose which devices are going to be permitted. There are so many device choices, so it is important to decide just what you mean when you say "bring your own device." You may really mean bring your own iPad but not your other tablets? With the increasing excess of devices out there that's continuously growing, it's important your list is as detailed as necessary, including types of smart phones and/or tablets, operating systems, models, etc.

Make sure the mobile devices you are allowing are equipped with the features you require. Decide what the minimum device requirements are and why. Be specific and state why you chose to support certain devices and exclude others. Let your users know what to expect before they bring in their devices.

3. Define Support

We've all had issues come up with mobile devices. To prevent your IT staff from being swamped with users requesting help, you can define a policy specifically for your BYOD mobile devices. Determine what you think your IT staff will be able to handle in terms of support.

You may decide to require your students to cover all the support and maintenance themselves or offer your IT staff up for certain small issues. Whatever you decide just be as specific as possible. Addressing things like this and any other potential problems you think might come up can prevent misunderstanding later on when questions start popping up.

4. Provide Clear Disclaimers Regarding What the School is Responsible For and Not Responsible For

Inevitably students' mobile devices will get lost, damaged, or even stolen while on school grounds. That's why it is important to state exactly whom is responsible for what. Let users know in advance so when the issue arises they know what to expect and you can avoid any possible disputes.

5. Don't Forget the Written Agreement

You can lay out all these great rules, requirements, and expectations, but you need to have every single user sign the written agreement to seal the deal. This includes all teachers and staff and well as students. Having parents sign too is also a good idea since more than likely they are the ones providing the devices. So make sure you not only provide everyone a copy of the policy, but also require a signed written agreement for them to get BYOD access. Having the written BYOD policy acknowledgement agreement signed will not only protect your school but also prevent misunderstandings about the BYOD policy and expectations.

6 Outline Acceptable Use and Violation Consequences

Everyone needs to know the acceptable use policies as well as the consequences for breaking these rules. This is where you should state that the devices are to be used as learning tools, not for entertainment. Describe what users are and aren't allowed to access while on school grounds.

Provide statements of clear consequences for student failure to follow the acceptable use policy and BYOD guidelines. Consequences could be the loss of access for a period of time. Be as specific as possible to make sure everyone is well-informed and knows exactly what to expect.

7 Decide on Whitelisted and Blacklisted Apps

There's a lot to consider when it comes to apps. You must decide what apps will be allowed or banned otherwise called whitelisting or blacklisting apps. A BYOD policy should explain that IT has the authority to prohibit the use of certain apps that might threaten the security of the school. Also, make sure your critical learning apps are secure and segregated on the devices.

8. Define the Device Enrollment Process

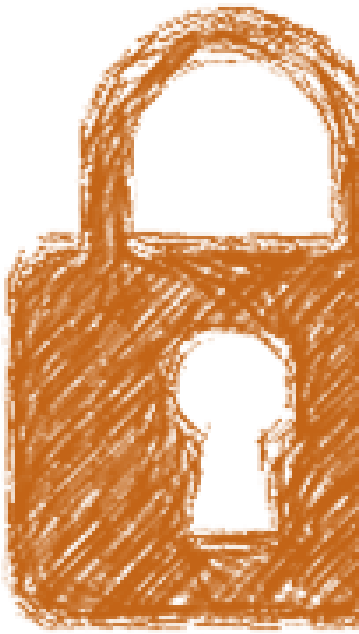
Consider on what factors you will block devices from connecting to your network. Make sure it is clearly stated in your policy that BYOD devices must be registered and authenticated before they connect to the school wireless network. This allows network administrators to detect unauthorized devices on the network.

9. Regular Reviews of Policies and Agreements are Essential

It's important to stay informed of what other schools/school districts are doing for their BYOD policy. Working on your BYOD policy is not a one-time thing and then you're done. As time goes by, you will probably need to revise your own policy, solicit internal feedback /comments, and publish a new version. Devices and apps constantly change, so plan on reviewing your policy at least once a year and having users sign and acknowledge any amendments.

10 Define Security Policy Procedures

BYOD has an inherent security risk. When students are allowed to take devices home or bring their own devices from home, there's an increased chance of malware infection. Therefore, maintaining security in a BYOD environment becomes more challenging for IT.



Your IT Staff needs to have a big role in the implementation of any BYOD policy, especially with security. When it comes to the security policy there's a lot to consider. Obviously you will have to determine the minimum BYOD security requirements for devices to be allowed access to your schools wireless network. You could have a separate network for student BYOD devices allowing access to the internet only and no other network resources. The use of antivirus apps, other security software and firewall settings should be covered in your BYOD policy as well.

11 Determine a Plan for Student Who Don't Have a Device

Even though most of today's students already have the devices necessary for BYOD, you still may have at least some who do not. You need to consider the possibility that some parents may not be willing or able to purchase a device for their student to use in the schools' BYOD program. Also consider the protocol for student who forget their device at home.

>>In Higher Ed. the average is 3-5 mobile devices per student.

>>In K-12 the average is 2 mobile devices per student.

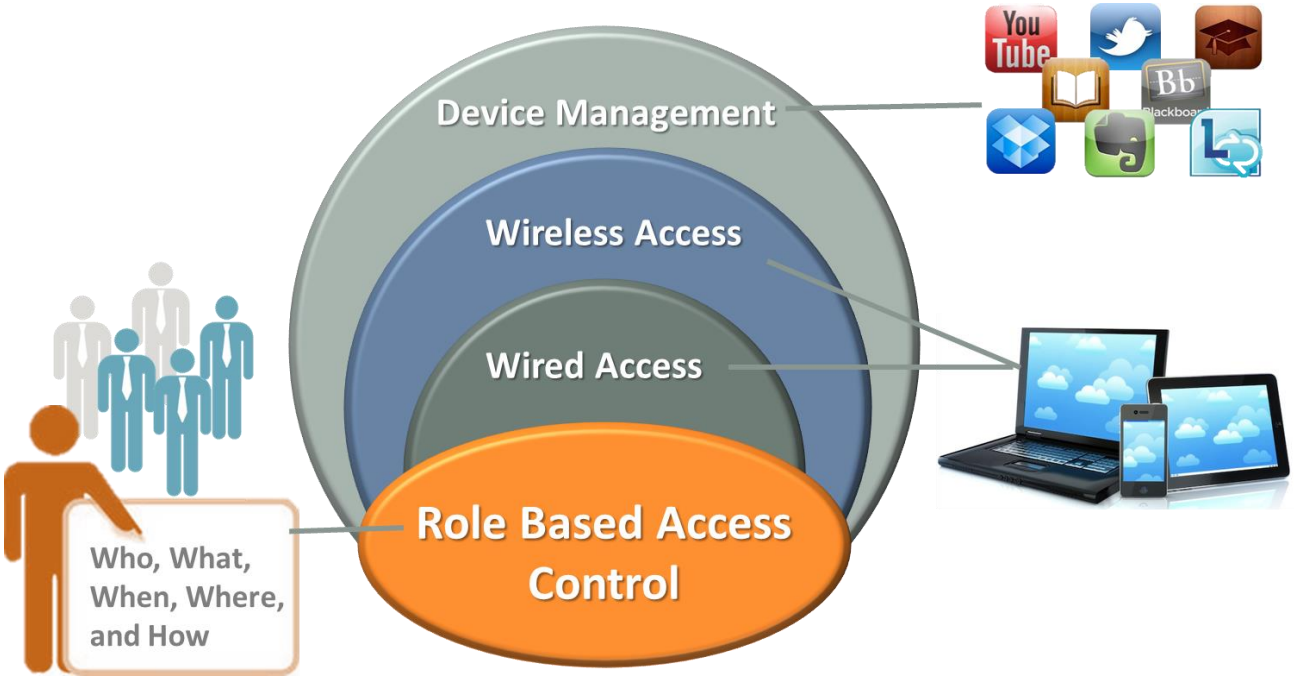
One possible solution for dealing with this issue is to purchase start a technology leasing program for your school where students check-out or rent devices. Buying a few carts full of devices is still going to be significantly cheaper than purchasing one for every student. There are also some other options like sponsorship, donation programs, etc. Come up with a plan for how you will deal with this and make sure to address it in your BYOD policy.

CHAPTER 3

BYOD SECURITY ENFORCEMENT & SUPPORT

Security is Foundation for BYOD

The biggest problem with BYOD and the reason most schools have never allowed it in the past is of course security. If schools did allow someone onto their network with their personal device, they didn't have an effective way to limit what they did on the schools wireless network.



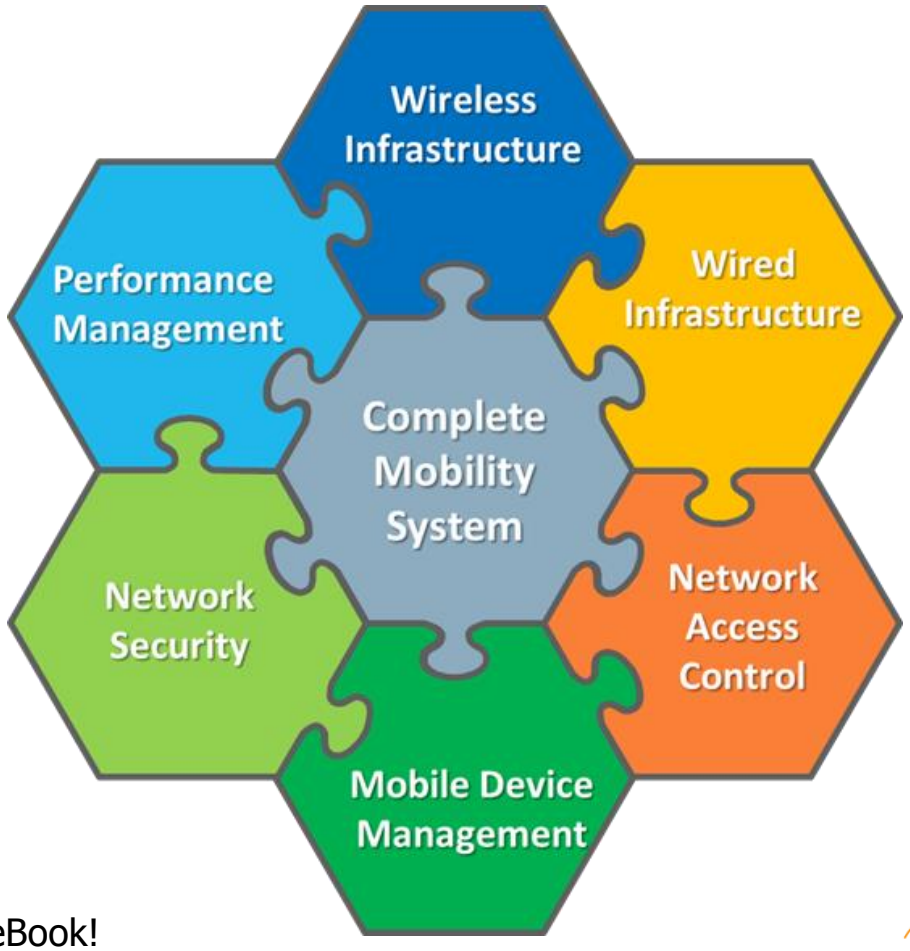
Security is a big challenge- unless the system is built on what we call "Role Based Access Control". Simply put, it's knowing who, what, when, and how people are connecting to the network, and having the ability to limit their access based upon that profile. Role Based Access Control is the foundation to allow BYOD.

Share this eBook!

securEdge networks
SecurEdgeNetworks.com

Mobility Systems Vs. Segmented Products

When preparing your school for a secure BYOD solution, although security is the foundation, there are many campus needs that must be considered. Traditionally schools thought of networking or security components separately. But with BYOD a holistic approach is needed, so a lot of planning is required on the front end to have a successful and secure BYOD solution for your school. Although every schools BYOD policy is different there are certain components all school wireless networks should have to support BYOD with the upmost performance and security.



A secure BYOD solution is like a puzzle. All the components (pieces) are connected to one another and they need each other to function and build the complete mobility system.

To sum it up, in order to support BYOD you'll need to Think Systems, not Products. Creating a clear BYOD Security Policy that covers all aspects of your wireless network infrastructure and current classroom technology will help you avoid any technology initiative failures.

CHAPTER 3

HOW WE CAN HELP

SecurEdge Networks

Who We Are

SecurEdge Networks is a specialty IT Solutions Provider focused on mobility and security. We've worked with hundreds of organizations to implement secure BYOD programs.

How we Help

Analyze: A thorough discovery of your current environment and your objectives.

Plan: Our design recommendations are based upon your end goal, as well as industry and solution specific knowledge.

Deploy: We can deploy BYOD solutions turnkey or we can work alongside your team to provide guidance on best practices.

Support: We offer managed services and custom support services to ensure the success of your BYOD program.

Share this eBook!

securedge networks

SecurEdgeNetworks.com

Get Started With BYOD

SecurEdge has helped hundreds of organizations implement BYOD programs. Register here to talk to one of our mobility consultants about best practices to support BYOD at your school.

Share this eBook!

securedge networks
SecurEdgeNetworks.com