BYOD Readiness Checklist for School Districts

Before you open the school doors to student and staff-owned devices,
use the checklist below to evaluate your school's readiness for BYOD.

Acceptable Use Policy

*When can students use devices? To do what?
To go where?*

The starting point for any school wishing to embrace BYOD starts with defining your Acceptable Use Policy. Which mobile devices and applications will you allow and which will you deny? Are students allowed to access social networks? What about text messaging?

Network Protection

Can we protect our network and student devices?

Do you have a solution that protects your network from malware and unauthorized content? Do you have anti-virus, URL filtering, secure remote access, and data protection in place?

Secure Network Access

Who is allowed to get on the network? How is it enforced?

A secure network requires authentication procedures that will allow you to enforce the Acceptable Use Policy. Can you protect your network from outside users? Will you allow off-campus access to the school network?

Network Capacity

Can our network handle multiple devices per student? Can it support high bandwidth applications?

BYOD devices are mobile by nature and most students will need to access the wireless network from multiple points on campus. Is your wireless network up to the challenge? Can it accommodate mobile traffic during peak times, such as the beginning of a class period? Can it handle the bandwidth required for multimedia applications?

Mobile Device Limitations

Where can students access real computers?

Tablets, smartphones, and other mobile devices are designed to supplement, not replace, the work done on "real" computers. There will be times when staff and students require a keyboard, a file structure, a larger screen, or access to software programs that are not supported on mobile devices.

Usability

Can we deliver education apps across all devices?

What are the critical education applications that your students rely on? Can you deliver these applications across all devices and operating systems? Consider a central location where all applications can be easily accessed.

Curriculum

Is the curriculum ready for BYOD?

A BYOD program requires a significant amount of curriculum analysis and redesign in order to take full advantage of mobile device features. How will you support teachers with rethinking their curriculum? Is there a place in the curriculum for digital citizenship?

*Digital Transformation
Toolkit Sponsored by
www.shi.com*

Professional Development

Are teachers ready for BYOD?

The success of a BYOD program relies heavily on the teachers who implement it. Do you have a plan for offering continued support to train teachers with BYOD implementation? How will teachers learn about new software applications and devices? Will you require all teachers to participate in BYOD?

Logistics

Have you considered the daily details?

There's much more to BYOD than simply allowing student devices at school. Where will students charge their devices? How will devices be secured when not in use, for example during sports or lunchtime? Do you have a plan for loaning equipment to students without a device?

Communication

Is everyone on board?

Frequent and ongoing communication between district administrators, staff, students, and parents is key. How will you involve parents in the planning and decision making process? Do you have a plan for keeping them involved in the program? Do parents know how the devices are being used at school and how they can follow-up at home?

Budget

Have you considered all the costs?

At first glance, a BYOD program may appear to save money by passing the cost of devices on to parents. However, there are many costs associated with BYOD implementation that must be considered. Is there room in the budget for network updates, loaner device purchase and repairs, school-owned computers, mobile device charging stations?

Guest Management

Can I extend network permissions to visitors and guests?

Does your network provide for guests? Can you ensure that guest devices coming onto the network have the freedom to access the resources required while protecting sensitive student data?