

DPS Bring Your Device to School (BYDS) Program Guidelines December, 2012

THE VISION, PLAN, AND SCOPE

The vision of the Durham Public Schools (DPS) 21st century learning is to provide 1:1 access for all students at all grade levels. Unfortunately, budget and technical constraints exist, making it a challenge to achieve. However, the Bring Your Device to School (BYDS) Program is a “bridge” to achieving the benefits for engaged students using technology devices in the classrooms until the technology marketplace can provide devices that are affordable in the K-12 environment and budgets allow for the district to provide for each student device. In short, the BYDS is the K-12 environment’s “survival technique” until such time as the marketplace can provide a cost-efficient device for K-12.

DPS is committed to providing an excellent 21st century teaching and learning environment for its students and faculty. To augment the gap of where DPS is today and the 1:1 vision for all students, DPS will begin the technology program of Bring Your Device to School (BYDS), starting with high schools and middle schools at the beginning of the 2013-14 school year.

Expansion of the BYDS Program into elementary schools will be evaluated in the 2013-14 school year.

DEFINITION OF A PERSONAL TECHNOLOGY DEVICE

A Personal Technology Device (PTD) is a portable Internet-accessing device designed to share information, record sounds, process words, and/or capture images, such as a laptop, tablet, smart phone, PDA, or eReader.

GENERAL EDUCATIONAL USAGE

DPS elects to standardize on Internet-based educational applications and platforms using Web 2.0 tools and collaborative programs, which makes DPS devices able to take on an agnostic nature. In simple terms, as long as the teacher-led application or tool is Internet-based, any device that can access the Internet can be used. This enables a wider ability for DPS students to take advantage of the program.

The number one rule for students in the BYDS Program is the teacher has the absolute final say as to whether or not the devices can and will be used in his or her classroom.

Therefore, the following usage guidelines are in place:

1. Students must obtain teacher permission before using a PTD during classroom instruction.
2. Student use of PTD must support instructional activities currently occurring in each classroom and lab.
3. Students must turn off and put away PTD when requested by a teacher.
4. Students should be aware that their use of the PTD could cause distraction for others in the classroom, especially in regards to audio. Therefore, audio should be muted, since headphones should not be used during the instruction time, unless directed by the teacher.
5. Students may use their PTD before school, at lunch, and after school only at the discretion of the school principal. The PTD should be used for educational purposes during these times also. If an adult asks a student to put his/her PTD away because of games or other non-instructional activities during these times, the student must comply.
6. Students will not do anything to disable the Child Internet Protection Act (CIPA) filter that the district maintains and runs on the BYDS wireless broadcast.
7. Students must comply with the Board Policy 3040 – Technology Acceptable Use and Board Policy 4301 - Code of Student Conduct (Sections I.9 and II.12).

CONSEQUENCES OF GENERAL USAGE

If students refuse to comply with the above guidelines, the following consequences will apply. Student infractions are:

1. First Offense – PTD will be confiscated until the end of the school day, when the student may retrieve it.
2. Second Offense – PTD will be confiscated until the end of the day, when the student's parent must retrieve it.
3. Third Offense – Loss of PTD privileges for a nine-week period of time.

CONSEQUENCES OF UNACCEPTABLE USE

If a school employee suspects that a student has violated the acceptable use policy of the district as identified in Board Policy 3040 – Technology Acceptable Use Policy (AUP), the personal PTD can be confiscated and the storage contents reviewed by school district staff. The PTD may be held for a reasonable amount of time while authorities review the storage contents. All violations of the AUP policy will result in the immediate loss of personal PTD privileges, parent contact, and additional school or legal consequences.

DEVICE SECURITY RISK

Technology security is taken very seriously within the District. PTDs are especially vulnerable to loss or theft. The PTD has financial value and may also have valuable and personal data on the device. It is imperative that the student who participates in the BYDS Program understands that the device must be secured in order to prevent theft. Here are the practices DPS requires of its students who participate in the BYDS Program:

1. The student must be aware of the security risks involved with their PTD. They must be aware that there may be others who would steal their device;
2. The student must understand and adhere to physically securing their PTD while on school property and when traveling to and from school; and,
3. The student must maintain an access control mechanism on their PTD.

1. STUDENT RESPONSIBILITY TO PROTECT THEIR PTD

DPS does not accept responsibility for personal property brought to the school by students. This includes any PTDs. Students who choose to bring their PTD to school assume total responsibility for the device. PTDs that are stolen or damaged are the responsibility of the student and their parents or guardian.

Students shall take all reasonable steps to protect against the theft or damage of their PTD.

2. PHYSICAL SECURITY

Students should take the following physical security preventative measures.

- a. Students should never leave the PTD unattended for any period of time. When not using the PTD, it should be locked in the school locker. PTDs left unattended will be picked up by staff, if found, and turned into the Technology Specialist or Media Center.
- b. Students should never leave the PTD in view of an unattended vehicle.

3. ACCESS CONTROL AND AUTHENTICATION

Students can only access the Internet via a wireless connection using a special band of wireless broadcast by the district especially created for BYDS devices.

Any student found connecting his or her PTD to the network using an Ethernet cable plugged in a wall jack will have his or her PTD confiscated and lose personal access privileges.

Students shall only use their PTD on the DPS BYDS wireless broadcast. At no time shall a student be allowed to use their own 3G/4G wireless connection to the Internet; the BYDS broadcast is filtered to comply with the Child Internet Protection Act (CIPA). Students are expected to follow the AUP when accessing the Internet through any device.

Students should not access the Internet through any cellular data provider while on campus. If a staff member sees a student accessing a website that is typically blocked from the DPS network, they must immediately take the device away and remediate the access.

STUDENT TROUBLESHOOTING OF THEIR PTD

Each student must understand basic troubleshooting of their device. The teacher, the technology specialist at the school, or the IT technician will not have the responsibility to troubleshoot connectivity or application issues on a student's PTD. Each student should maintain their own device manufacturer's maintenance and support vehicle as well as their "How to" booklet for their device. Student troubleshooting of their PTD should take place outside of the instructional day. At no point shall instruction time stop so that a student can troubleshoot their PTD in the classroom.

TECHNICAL RAMIFICATIONS OF A BYDS PROGRAM

There are several technical ramifications that a BYDS Program brings to the technology department. Those ramifications relate to the areas of wireless service and support and PTD support.

In order to support the BYDS Program, the Information Technology (IT) Division must implement a Network Management System (NMS) that includes a Network Access Control (NAC) component for its existing wireless service. It is the goal of the IT Division to provide:

1. A secure wireless broadcast especially designed for BYDS, which is Internet access only.
2. The NMS and the NAC implementation must provide for supporting the wireless connectivity of many different types of devices.
3. The NAC must allow for auto registering of the student's PTD devices. The administration of the MAC addresses by the school technology staff is not able to handle the load of a manual registration process.
4. The monitoring of the wireless service must be enhanced in order to advance the proactive management of the wireless service.
5. The PTDs will not be supported by the IT Department.

ENSURING THE PROGRAM DOES NOT EXPAND THE DIGITAL DIVIDE FOR OUR COMMUNITY

Many BYDS programs, if they are not careful, can increase the digital divide of its district's community. Therefore, it is imperative, that the DPS continues its expansion of 1:1 technology programs and continue to expand DPS' minimum technology baseline standards to ensure an adequate student to computer ratio for all classrooms. The BYDS Program is not a replacement for continuing to achieve its 1:1 vision.