Instruction

Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct [1]

The Superintendent or designee shall establish a *Bring Your Own Technology* (BYOT) *Program*. The program will: [2]

1. Promote educational excellence by facilitating resource sharing, innovation, and communication to enhance (a) technology use skills; (b) web-literacy and critical thinking skills about Internet resources and materials, including making wise choices; and (c) habits for responsible digital citizenship required in the 21st century. [3]
2. Provide sufficient wireless infrastructure within budget parameters. [4]
3. Provide access to the Internet only through the District's electronic networks. [5]
4. Identify approved BYOT devices and what District-owned technology devices may be available; e.g., laptops, tablet devices, E-readers, and/or smartphones.
5. Align with Board policies 4:140, *Waiver of Student Fees*; 5:120, *Employee Ethics; Code of Professional Conduct; and Conflict of Interest*; 5:125, *Personal Technology and Social Media; Usage and Conduct*; 5:170, *Copyright*; 6:120, *Education of Children with Disabilities*; 6:235,

---

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[1] This policy is optional. It concerns an area in which the law is unsettled. This policy contains an item on which collective bargaining may be required. Any policy that impacts upon wages, hours, and terms and conditions of employment, is subject to collective bargaining upon request by the employee representative, even if the policy involves an inherent managerial right. Consult the board attorney and the district's information technology professional(s) for advice to create a legally sound program that fits your district's mission statement for instruction.

[2] Customize paragraphs 1-8 to reflect the how the program will align with the board's mission statement for instruction and goals for its program.

[3] 105 ILCS 5/27-~~4101~~3.3, renumbered by P.A. 104-391 and scheduled for repeal on 7-1-27; 5/27-405, added by P.A. 104-391, and 47 C.F.R. §54.520(c)(1)(i) require Internet safety instruction. See f/n 24 in 6:60, *Curriculum Content*, for more discussion.

[4] Districts may want to consider a *guest network*, similar to what hotels and other service industry hosts provide to their customers. This can protect a district's network from malicious software, which is discussed in f/n 5 below.

[5] Care must be taken to comply with the Children's Internet Protection Act (CIPA) (47 U.S.C. §254). CIPA requires the district to provide content filters, blocking lists, or district monitoring of Internet website traffic for patterns of usage that could indicate inappropriate network usage. While a program using district-owned technology devices is always subject to the district's electronic network rules, a BYOT program creates the possibility for students to bypass the district's electronic network and access the Internet through their own wireless providers' signals. This *bypass* complicates a district's duty under CIPA because it cannot guarantee students use its electronic network; preventing bypassing is hard for school officials to control.

Consult the board attorney about managing CIPA compliance issues in the context of a BYOT program. This sample policy is conservative, and it requires that CIPA govern the use of any BYOT device's Internet access capability while the device is at school. If the board will allow a student to bypass the district's electronic network and access his or her wireless providers' signals, consult the board attorney.

Care must also be taken to reduce the electronic network's vulnerability to malicious viruses and malware. Malicious viruses and malware ~~are increasingly being~~ may target~~ed to~~ smartphone users through spam text messages. ~~This is evidenced by the Federal Trade Commission (FTC) filing lawsuits around the country accusing companies of ordering or engineering the sending of hundreds of millions of spam text messages to mobile phone users.~~ The district may want to require students to ensure their BYOT devices contain an anti-virus and/or anti-malware software product. While many of these software products are free, some are not. Requiring all BYOT devices to have this type of software presents equity issues between students because it may require parents/guardians to spend funds to participate (see the discussion at~~in~~ f/n 6 below).

Access to Electronic Networks; 7:140, *Search and Seizure*; 7:180, *Prevention of and Response to Bullying, Intimidation, and Harassment*; 7:190, *Student Behavior*; 7:340, *Student Records*; and 7:345, *Use of Educational Technologies; Student Data Privacy and Security*. [6]

6. Provide relevant staff members with BYOT professional development opportunities, including the provision of: [7]
    a. Classroom management information about issues associated with the program, e.g., technical support, responsible use, etc.;

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[6] A BYOT program must continue to follow established policies. Boards may use this alternative, "Align with established Board policies."

Managing the following board policy issues may require a consultation with the board attorney:

1. 4:140, *Waiver of Student Fees*, needs examination because most BYOT programs require parents/guardians to spend funds to participate. 105 ILCS 5/10-20.13, amended by P.A. 104-391~~s 102-1032 and 102-805, eff. 1-1-23~~, requires districts, at a minimum, to waive charges for textbooks, instructional materials, and other fees for children whose families are unable to afford them. See also policy 6:210, *Instructional Materials*, stating that district classrooms and learning centers should be equipped with an evenly-proportioned, wide assortment of instructional materials, including textbooks, workbooks, audio-visual materials, and electronic materials.
2. Management issues concerning 5:125, *Personal Technology and Social Media; Usage and Conduct*, and 5:170, *Copyright* are discussed in f/ns 7 and 8 below.
3. 6:120, *Education of Children with Disabilities*, requires consideration for students with disabilities when integrating any technology programs into the educational environment. As with district-provided devices (often referred to as 1:1 *technology programs*), devices must be accessible to students with disabilities, including those who are blind, have low vision or have a disability that affects their ability to access print information. The use of mobile devices that do not allow a student with a disability to access the instructional materials would be a violation of the student's right under the Individuals With Disabilities Education Act (IDEA) (20 U.S.C. §1400 et seq.).
4. 6:235, *Access to Electronic Networks*, is discussed in f/n 5 above.
5. 7:140, *Search and Seizure*, still applies in a BYOT program. The Fourth Amendment protects individuals from searches only when the person has a legitimate expectation of privacy. However, 105 ILCS 5/10-22.6(e) allows school officials to inspect the personal effects left by a student on property owned or controlled by the school, e.g., lockers, desks, and parking lots. Many cases suggest that to search a student's possessions left in the locker, school officials need individualized suspicion of wrongdoing. Many of the issues re: the search of electronic devices that are discussed in 7:190-AP6, *Guidelines for Investigating Sexting Allegations*, will apply to investigations involving BYOT devices. To minimize mediating with law enforcement for parents/guardians about confiscated devices, districts should distinguish whether they are acting upon their own initiative or need to contact law enforcement. See f/ns in sample policy 7:140, *Search and Seizure*, and the policy's **Seizure of Property** subhead.
6. 7:180, *Prevention of and Response to Bullying, Intimidation, and Harassment*, and 7:190, *Student Behavior*, present similar issues to #3 and #4 above. Students must be aware that traditional expectations for appropriate behavior, and the consequences for inappropriate behavior, apply to a BYOT program.
7. See 7:340, *Student Records*. The law is not clear whether materials created by students participating in a BYOT program through a district's network access are *school student records*.
8. 7:345, *Use of Educational Technologies; Student Data Privacy and Security*, requires districts to comply with the Student Online Personal Protection Act (SOPPA), 105 ILCS 85/~~, amended by P.A. 101-516~~; see also 23 Ill.Admin.Code Part 380. Implementation of a BYOT program does not exempt a district from complying with SOPPA's contractual and security mandates, including implementation and maintenance of reasonable security procedures and practices designed to protect student's *covered information*. Reasonable security practice guidance adopted by ISBE recommends, in part, that districts create a separate wireless network for personal or untrusted devices. See sample policy 7:345, *Use of Educational Technologies; Student Data Privacy and Security*, at f/n 11 for more information.

[7] See f/n 1 above re: collective bargaining. Moving forward without properly training educators to manage BYOT issues may create pedagogical problems. One option for this training is to incorporate it into the training required during the in-service on educator ethics, teacher-student conduct, and school employee-student conduct required by board policy 5:120, *Employee Ethics; Code of Professional Conduct; and Conflict of Interest*. Many issues involved in BYOT programs intersect with maintenance of appropriate behavior and policy 5:125, *Personal Technology and Social Media; Usage and Conduct*.

b. A copy of or access to this policy and any building-specific rules for the program;
c. Additional training, if necessary, about 5:170, *Copyright*; and
d. Information concerning appropriate behavior of staff members as required by State law and Board policy 5:120, *Employee Ethics; Code of Professional Conduct; and Conflict of Interest*. [8]

7. Provide a method to inform parents/guardians and students about this policy.
8. Include the program in the annual report to the Board as required under Board policy 6:10, *Education Philosophy and Objectives*.

The District reserves the right to discontinue its BYOT program at any time. The District does not provide liability protection for BYOT devices, and it is not responsible for any damages to them.

Responsible Use [9]

The District recognizes students participating in the program as responsible young adults and holds high expectations of their conduct in connection with their participation in the program. Teachers may encourage students to bring their own devices as supplemental in-class materials when: (a) using the devices will appropriately enhance, or otherwise illustrate, the subjects being taught; (b) the Building Principal has approved their use and found that their use is age-appropriate; and (c) the student's parent/guardian has signed the *Bring Your Own Technology* (BYOT) *Program Participation Authorization and Responsible Use Agreement Form*. A student's right to privacy in his or her device is limited; any reasonable suspicion of activities that violate law or Board policies will be treated according to policy 7:140, *Search and Seizure*.

Responsible use in the program incorporates into this policy the individual's *Acceptable Use of Electronic Networks* agreement pursuant to Board policy 6:235, *Access to Electronic Networks*. Responsible use also incorporates the established usage and conduct rules in Board policies~~y~~ 5:125, *Personal Technology and Social Media; Usage and Conduct*, for staff, and 7:190, *Student Behavior*, for students. Failure to follow these rules and the specific BYOT program student guidelines may result in: (a) the loss of access to the District's electronic network and/or student's BYOT privileges; (b) disciplinary action pursuant to Board policies 7:190, *Student Behavior*; 7:200, *Suspension Procedures*; or 7:210, *Expulsion Procedures*; and/or (c) appropriate legal action, including referrals of suspected or alleged criminal acts to appropriate law enforcement agencies.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[8] 23 Ill.Admin.Code §22.20 and 105 ILCS 5/21B-75~~, amended by P.A. 102-552~~.

[9] This section provides general guidelines. A BYOT program will require a parent/guardian authorization to participate in it and specific guidelines for students. See sample exhibits 6:220-E1, *Authorization to Participate in the Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct Agreement*; 6:220-E2, *Bring Your Own Technology (BYOT) Program Student Guidelines*; and 6:235-E5, *Children's Online Privacy Protection Act*. See f/ns 7 and 8 above re: teachers' guidelines. See f/n 1, above discussing how the application of additional guidelines for teachers may have collective bargaining implications.

LEGAL REF.: 15 U.S.C. §§6501-65068, Children's Online Privacy Protection Act; 16 C.F.R. Part 312, Children's Online Privacy Protection Rule.
20 U.S.C §6751 et seq.7101, Every Student Succeeds ActEnhancing Education Through Technology Act.
47 U.S.C. §254(h) and (l), Children's Internet Protection Act.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
105 ILCS 5/10-20.28.

CROSS REF.: 1:30 (School District Philosophy), 4:140 (Waiver of Student Fees), 5:120 (Employee Ethics; Code of Professional Conduct; and Conflict of Interest), 5:125 (Personal Technology and Social Media; Usage and Conduct), 5:170 (Copyright), 6:10 (Educational Philosophy and Objectives), 6:40 (Curriculum Development), 6:120 (Education of Children with Disabilities), 6:210 (Instructional Materials), 6:235 (Access to Electronic Networks), 7:140 (Search and Seizure), 7:180 (Prevention of and Response to Bullying, Intimidation, and Harassment), 7:190 (Student Behavior), 7:340 (Student Records), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)