

## Instruction

### **Exhibit - Bring Your Own Technology (BYOT) Program Student Guidelines**

*This exhibit accompanies policy 6:220, Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct. It should be sent home with students along with 6:220-E1, Authorization to Participate in the Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct Agreement, and 6:235-E5, Children's Online Privacy Protection Act. It outlines BYOT guidelines. Building Principals may want to include this in the student handbook. Modify this exhibit to reflect the District's and any building-specific guidelines.*

The purpose of the District's BYOT program is to extend and enrich the learning environment. The following guidelines apply to students who participate in the program:

- Access only the District's Internet gateway. The District filters access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate at school pursuant to policy 6:235, *Access to Electronic Networks*. Make no attempts to bypass the District's Internet gateway. Similar to when a filter is disabled or malfunctions, it is impossible to control all Internet material, and a BYOT participant may discover inappropriate material. It may also be discovered if and/or when sharing a BYOT device with another student. Report inappropriate content and conduct to your classroom teacher.
- Follow the standards of your parents/guardians. The District respects each family's right to decide whether or not to participate. District-provided technology may be an alternative.
- Access only authorized data or files on the computer or Internet sites that are relevant to the classroom curriculum and suggested by a teacher. Students are strictly prohibited from infecting the District's network(s) with a virus or malware program designed to damage, alter, destroy, or otherwise compromise the network, and hacking, altering, or bypassing security policies or measures. Installing and updating anti-virus and anti-malware software and keeping the operating system on BYOT devices updated is required. The District may examine any BYOT device that it suspects is causing network problems or may be the source of an attack or virus infection.
- Use of a BYOT device is subject to policy 7:190, *Student Behavior*.
- Transmit only appropriate content while using the District's electronic network. At no time, may a photographic image or video of any person on campus be made, posted, or shared, unless authorized by the teacher for instructional purposes. Any reasonable suspicion of an activity that violates law or Board policies will be treated according to policy 7:140, *Search and Seizure*. Bullying, harassment, or sexual material will not be tolerated and will be managed pursuant to policies 7:180, *Prevention of and Response to Bullying, Intimidation, and Harassment*, or 7:20, *Harassment of Students Prohibited*, as appropriate. Retrieval of devices that become involved in a law enforcement investigation is the student and parent/guardian's responsibility.
- Charge all BYOT devices prior to school every day. Turn off and keep BYOT devices in the sight of the teacher during assessments, unless otherwise directed by a teacher. Immediately follow any teacher's instruction to shut down BYOT devices or close the screen. All BYOT devices must be in silent mode and put away when directed by teachers.

Sharing BYOT devices with other students is allowed only when a parent/guardian has approved this in writing through the *Bring Your Own Technology (BYOT) Program Participation Authorization and Responsible Use Agreement* and the teacher has directed it.

Adopted: 5/28/2013

Revised: 7/17/2018, 07/25/2023