

BRING YOUR OWN DEVICE (BYOD)**I. Introduction**

In compliance with Florida law and in order to ensure a safe, focused learning environment, FSUS teachers and administrators may limit the use of and/or exposure to wireless communications devices and personal computers, hereafter referred to as personal electronic devices. When permitted by state law and the FSUS Student Code of Conduct, students may use their personal laptops to support their learning. This may include participating in instructional activities, accessing and saving information from the Internet, collaborating with peers, and using productivity tools or educationally appropriate apps approved for classroom use.

Formatted: Normal, Justified, Indent: Left: 0.5", No bullets or numbering

~~FSUS is committed to developing a technologically relevant and engaging learning environment for all students by providing them with the opportunity to develop the resource sharing, innovation, communication skills, and tools that are essential to both life and work in the 21st century. FSUS will offer a Bring Your Own Device (BYOD) option that allows students to wirelessly access the Internet for limited educational purposes as directed by a teacher or administrator. Students granted access to the district's network/Internet services from any device will be governed by FSUS's Acceptable Use Policy (School Board Policy 8.62), related administrative guidelines, and the Student Code of Conduct.~~

Formatted: Justified

II. Risks and Responsibilities

Any personal electronic device brought on campus will be governed by FSUS's Acceptable Use Policy (School Board Policy 8.62), related administrative guidelines, and the Student Code of Conduct.

Formatted: Justified, Indent: Left: 0.5", No bullets or numbering

A. For BYOD purposes, a device is any district provided or personally owned computer or electronic device including, but not limited to, phones, tablets,

Formatted: Justified

notebooks/laptops, wearables (e.g. Google Glass, smartwatches), iPod touches (or similar), and e readers.

~~B. With school or district staff approval, students may use their own devices at school to participate in instructional activities, access and save information from the Internet, collaborate with other learners and utilize productivity tools and instructionally appropriate apps loaded on their devices. Because personal devices will not be able to access internal district resources such as file and print servers, documents created should be saved to removable media such as flash drives or to a cloud storage location.~~

Internal Access Restrictions: Personal electronic devices will not have access to internal school or district resources such as print servers.

~~A. Students who choose to bring their personal devices may use the "FSUS-student" filtered wireless public network while on campus. When logging onto the "FSUS-student" wireless network, students will be required to accept the district's Acceptable Use Policy (AUP) for network access.~~
Network and Filtering: All FSUS networks are filtered for the safety of users in compliance with the Children's Internet Protection Act (CIPA) to ensure user safety requirements. Any attempts to by-circumvent-pass these safety filters or to "hack" into FSUS technology, and/or FSUS platforms, programs, and/or software are strictly in any way is expressly prohibited.

~~B. Internet Content Risk: Nevertheless, caregivers are advised that a-Despite filtering measures, it may be possible for determined users may be able to gain access to online content that may be inappropriate or objectionable.~~
By participating in the BYOD (Bring Your Own Device) program, parents acknowledge and accept this risk.

~~C. Network Access Limitations: Non-wireless (wired/Ethernet) access to the district network is not permitted for personal electronic devices.~~
Devices on the Internet that they and/or their caregivers may find inappropriate, offensive, objectionable, or controversial. Caregivers assume this risk by allowing their child to participate in the BYOD program.

D. Privacy Notice: Users should have no expectation of privacy regarding personal files or online activity while connected to the FSUS network. FSUS staff may review files or monitor activity at any time to ensure responsible use and protect system integrity. If there is a reasonable suspicion of policy violation, devices may be inspected and/or confiscated. Violations may result in disciplinary action, including loss of technology privileges or further consequences per the Student Code of Conduct.

C. —

D. — Non wireless access to the district's network, such as through Ethernet cable, by personal devices is prohibited. Know that users have a limited right to, nor should they have an expectation of, privacy in the content of their personal files and records of their online activity while on the district's network. Access to the "FSUS student" network is a privilege and administrators and faculty may review files and messages at any time to maintain system integrity and ensure that the users are acting responsibly. If reasonable belief exists that a student has violated the terms of this agreement, or other district policy, the student's device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may extend to loss of technology privileges and/or further action per the FSUS Student Code of Conduct.

III. Usage Expectations

A. Students must complete and submit a required BYOD form with parental signature before authorized to have a personal computer on campus.

B. Approved Areas: Personal electronic devices can only be used in designated or approved areas and students must comply with staff directives regarding the use of technology devices, as outlined in the Student Code of Conduct or in compliance with staff directives.

C. Disruption and Misuse: Using functions on electronic devices in anyUse of personal electronic devices in a manner way that disrupts the educational environment or violates the Acceptable Use Policy (AUP) will be subject result to ~~in~~ disciplinary action.

Formatted: Justified, Indent: Left: 0.5", No bullets or numbering

Formatted: Justified

Formatted: Normal, Justified, No bullets or numbering

Formatted: Justified

Formatted: Justified

~~D. Recording Restriction: Audio, photo, or image-video recording, whether through picture or video, directly related to a student without prior explicit permission of all consent of the individuals being recorded is strictly prohibited. Written parental consent is required for before any media is publication shed. Audio, photo, or video recording is allowable if the student's image is incidental or captured only as part of the background, or if a student is shown participating in school activities that are open to the public and without a specific focus on any individual.~~

~~E.~~

IV. Liability and Support

~~A. Use at Own Risk: Students bring personal electronic devices to school at their own risk. FSUS will not be held is not responsible if a device is for lost, stolen or misplaced devices, including those that may have been confiscated due to policy violations.~~

~~F.B. Moreover Limited Technical Support: FSUS will not not be responsible for provide technical support of personal electronic devices, beyond assisting with providing necessary district-specific connectivity and login access information.~~

~~II. Required Use of Personal Devices~~

~~Use of personal devices is never a requirement and will not impact student grades. In instances where a device is required for an assignment, students without a device of their own will be provided one by FSUS for use on campus.~~

STATUTORY AUTHORITY:

LAW(S) IMPLEMENTED:

STATE BOARD OF EDUCATION RULE(S)

HISTORY:

ADOPTED: 12/8/15

Formatted: Indent: Left: 0.5", No bullets or

Formatted: Justified

Formatted: Justified

Formatted: Justified

REVISION DATE(S):

FORMERLY: NEW