

**FLORIDA STATE UNIVERSITY SCHOOLS  
POLICY MANUAL  
AUXILIARY SERVICES  
CHAPTER 8.0**

**8.64**

**BRING YOUR OWN DEVICE (BYOD)**

**I. Introduction**

In compliance with Florida law and 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. Students may use personal electronic devices before or after school and not during the instructional day.

**Deleted:** in order

**Deleted:** When permitted by state law and the FSUS Student Code of Conduct, students may use their personal laptops to support their learning.

**Deleted:** 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.

**Deleted:** only

**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.

- A. **Internal Access Restrictions:** Personal electronic devices will not have access to internal school or district resources such as print servers.  
**Network and Filtering:** All FSUS networks are filtered in compliance with the Children's Internet Protection Act (CIPA) to ensure user safety. Attempts to bypass these filters or to hack into FSUS technology, platforms, or software are strictly prohibited.
- B. **Internet Content Risk:** Despite filtering measures, it may be possible for determined users to access 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.

- 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.

### 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, [such as cellphones](#), can only be used in designated or approved areas as outlined in the Student Code of Conduct or in compliance with staff directives. [Personal computers may only be used outside of the instructional day.](#)
- C. Disruption and Misuse: Use of personal electronic devices in a way that disrupts the educational environment or violates the Acceptable Use Policy (AUP) will be result in disciplinary action.
- D. Recording Restriction: Audio, photo, or video recording directly related to a student without explicit permission of all individuals being recorded is strictly prohibited. Written parental consent is required before any media is published. 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.

### IV. Liability and Support

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

B. Limited Technical Support: FSUS will not provide technical support of personal electronic devices beyond assisting with district-specific connectivity and login access.

**STATUTORY AUTHORITY:**

**LAW(S) IMPLEMENTED:**

**STATE BOARD OF EDUCATION RULE(S)**

**HISTORY:**

**ADOPTED:** 12/8/15

**REVISION DATE(S):** 11/18/25

**FORMERLY:** NEW