

BYOD 9-12

Falls City Independent School district aims to give more choice and flexibility to families and students in using technology for learning through the Bring Your Own Device (BYOD) program. This document outlines the requirements for Bring Your Own Device (BYOD) usage for 9th - 12th grade students enrolled at and attending Falls City Independent School District. Families may choose a Chromebook, laptop, tablet, or iPad that meet minimum specifications to use on campus for learning. Each student device will be assigned a unique passphrase managed by FCISD that will allow them to access CIPA level filtered District Wi-Fi. If the student's access has to be revoked for any reason it can be done so without disrupting other students' access.

BYOD Equipment Minimum Requirements

- Operating System – Windows 11, macOS, or ChromeOS that is automatically updated and patched through the OS setting. Operating Systems that are no longer patched and updated by the manufacturer due to age will not be allowed.
- Google – Ability to access Google Apps for education whether through a web browser such as Edge or Chrome.
- Wi-Fi – capable of connecting to a wireless network system (Wi-Fi) and with no cellular data connectivity
- End point protection – devices must have some form of protection against malicious activity such as anti-virus, malware, etc. Some examples are Microsoft Defender, Bitdefender, Norton, and Webroot.
- Battery – a minimum battery life of five hours
- Microphone and headphones – allows for the use of a microphone or headphones either through USB, aux jack, or Bluetooth.

Optional Features

- Built in cameras – allow for the use of video conferencing through Zoom or Google. Families may want to find a device that allows the camera to be covered when not in use or purchase a separate camera cover.

Phones and cellular connected devices are NOT BYOD devices and will not be assigned a passcode to access Wi-Fi.

Internet Filtering – When on campus and connected to FCISD Wi-Fi internet is filtered unless a bypass tool is being used to circumvent the filtering. BYOD devices are required to use the district Wi-Fi and must not use personal hotspots, cellular data, or VPNs to bypass filtering. If filtering is bypassed student access will be revoked.

How FCISD is keeping your student safe on the internet – FCISD uses two methods of internet filtering for all devices on the Student BYOD network. CIPA compliant filtering provided by Lightspeed Systems as well as filtering defined at the firewall level.

User Responsibilities

- Ensuring end point protection such as anti-virus is installed and regularly updated
- Secure your device with a password or PIN when not using and keeping that password or PIN private to prevent use by others.
- FCISD will provide basic technology support for devices such as connecting them to the Wi-Fi or connectivity issues with Google Apps and minor hardware issues such as keyboard or mouse malfunction. Any major hardware issues will need to be resolved by the family. It is suggested that you purchase a warranty for your device.
- Printing will not be supported when using the district Wi-Fi. Please plan to either print at home or submit your assignments through email or Google apps.
- The student is responsible for keeping track of their device and not loaning it out to others.
- If a device is infected with virus or malware, it will be removed from the Student-BYOD Wi-Fi until the user can clean the device.
- Bring the device to school fully charged. Charging in the class cannot be guaranteed to be available.

Consequences vary and are at discretion of principal and technology.

Resources:

Children's Internet Protection Act (CIPA) <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>

Lightspeed Filtering <https://www.lightspeedsystems.com/blog/strengthen-your-protection-students-byod-iot-devices-lightspeed-filter/#>