

Bring Your Own Device Policy

Archbishop Stepinac High School is a “Bring Your Own Device” (BYOD) school. We believe this affords families the option to purchase a device which is best suited for their sons’ needs and their budgets

Required Device Specifications

All incoming freshmen are required to have a **Windows Device with touch screen capability***

Minimal Specifications:

- Windows 11 OS
- 16 GB of RAM or better
- Touchscreen with OneNote capability

**While other devices will work on the Stepinac network we are unable to support them and cannot guarantee your student will be able to access or take full advantage of the education applications used here at Archbishop Stepinac.*

Approved Devices:

- **Microsoft Surface Pro 9** or newer
- **Lenovo Yoga**
- **HP Writable Laptop**

Students will be permitted to use their devices for instructional purposes only (such as accessing textbooks and learning platforms, note-taking, research, collaboration, etc.). Teachers, in coordination with administrators, make the final decision for any instructional tools used in their classroom and will communicate their expectations to students and parents.

Students who BYOD must comply with the following requirements:

- Students may only access the internet using Stepinac's filtered "Student Wifi" wireless network. Internet access from outside sources, such as using a data plan associated with a personally-owned device, is strongly discouraged on school grounds. Stepinac will not take responsibility for content a student may access utilizing data from outside sources.
 - Students are prohibited from attempting to bypass Stepinac's firewalls and web filters. As such, the use of Virtual Private Networks (VPNs) is strictly prohibited.
 - The student takes full responsibility for his or her technology device. Stepinac is not responsible for the security or loss of student-owned technology. Students are strongly encouraged to lock up or securely store devices when not in use. Stepinac is also not responsible for any purchases that students make through an App store or a website.
 - The technology may not be used for academic dishonesty or non-instructional purposes.
 - The student may only access files, programs, or websites that are relevant to the classroom curriculum.
 - The student complies with teachers' requests to shut down the device or close the screen.
 - The student understands that bringing on premises or infecting the network with a virus, Trojan, or program designed to damage, alter, destroy or provide access to unauthorized data or information is in violation of the AUP and will result in disciplinary actions.
 - The student acknowledges that accessing information on the school's network via hacking, altering, or bypassing network security policies is a violation of the AUP and will result in disciplinary actions.
 - Stepinac has the right to collect and examine any device that is suspected of causing problems or being the source of an attack or virus infection.
-

BYOD Frequently Asked Questions

Will my child have access to the internet while using his/her device?

Students using their personal devices will be required to connect to Stepinac's Student Wifi wireless network. The school-provided WiFi network contains filtered internet access, per the federal and New York State laws. *While on school property, students should only use the Stepinac Student WiFi internet connection.*

As an important component of BYOD, students will receive instruction in appropriate and safe online behavior. In addition, access to the internet and its use shall be in accordance with school guidelines, the Student Acceptable Use Policy (AUP)

Will technical support be provided?

Technical support will be provided for network access and all Stepinac-provided platforms. Support for the physical device will not be provided. It is the responsibility of each student to care for his/her device and keep it in working order, including charging it outside of school.

What are the potential consequences of misuse?

Above all, Stepinac strives to maintain a safe and productive learning environment. Students are, therefore, expected to adhere to the policies, procedures, and guidelines established for safety and productivity at all school sites. Students who choose to ignore, circumvent or violate those efforts will face consequences. These consequences may include, but are not limited to revocation of BYOD privileges, confiscation of devices (to be returned to parents or guardians) or other discipline, as outlined in the Stepinac Student Handbook and AUP.