

J.H. Gunn

BYOT



We are pleased to announce that we have rolled out

Bring Your Own Technology at J.H. Gunn!

What is BYOT?

Bring Your Own Technology is a program which allows students to use their own technology at specified times during the day to enhance the learning experience. Examples of the types of technology which can be used are: laptops, eBook readers, tablets, Smartphones, etc.

BYOT Frequently Asked Questions

1. Can the Guest Network be opened only for staff and not students?

When we activate the guest network for a school, any device can get onto the guest network (student device, staff device, visitor device). The guest network cannot discern who the device belongs to. This network is filtered at the student level for anyone accessing it.

2. How do I access the Internet on the Guest Network?

Most devices will detect a wireless connection. Your device should prompt you to join an available network if there is a wireless connection near you. When prompted, choose the guest network (**CMSGuest478**). Once you choose this network and open an Internet browser, you will be prompted to accept the terms of service and abide by all District policies and procedures.

3. Why am I filtered on my own device?

Student and adult (unless bona fide research) filtering is a requirement of all public schools. The Children's Internet Protection Act (CIPA) requires all network access to be filtered, regardless of the device you use to access it while in a public school. The network you are using while at school belongs to CMS and will be filtered.

4. Will there be a permission form that needs to be signed before a student brings their own device to school?

There is no special permission form to be signed from the district perspective, but your school may require that you sign an agreement before you bring a device to school.

5. Will there be technical assistance provided to access the wireless network?

Since there are literally hundreds of devices that could be brought to school as part of the *BYOT* program, there is no technical assistance provided other than providing the name of the wireless connection. Students will be expected to know how to connect their devices.

6. If my device won't work, will someone from the school district fix the device?

It is not the responsibility of the CMS staff to fix/repair/troubleshoot individual devices. Check the owner's manual for issues that could arise or take the device to a computer repair shop.

7. How will students be using devices as part of their academic work at school and home?

Your child's teacher will be letting you know how they plan to integrate the utilization of devices into their teaching and learning environment in the classroom.

8. I brought my device to school and my teacher will not allow me to use it, what do I do?

The teacher has the final say on classroom procedures. If your teacher asks you not to use your device, you should follow their instructions. Although access is available, it is not guaranteed for every classroom situation.


9. If a teacher is delivering a lesson that uses devices, will my child be at a disadvantage if they do not have one?

No - there will be school or district provided devices available, or your child may be able to share with a classmate who brought a device to school.

10. How will an administrator have the ability to revoke a students' *BYOT* privilege?

If a student is not following the developed guidelines for the use of his or her personally owned device, an administrator can revoke the privilege through the regular discipline process.

11. How can a teacher or staff member tell if a student is using a 3G/4G wireless connection to the Internet rather than the school division's wireless access?

While it can be difficult to tell at times, if a staff member sees a student accessing a website that is typically blocked from the CMS network, the student is likely on 3G/4G connection. If the student is connected to a wireless network the  symbol will be displayed. The quickest way to help enforce this is by observing what students are accessing.

12. I have a data plan from a provider (AT&T, Sprint, Verizon etc.) on my digital device that allows internet access without using the CMS student access. Is this allowable?

Students are expected to follow the AUP when accessing the internet through any device. Students should not access the internet through any cellular data provider while on campus.

13. Am I still held accountable for the Acceptable Use Policy I accepted at the beginning of the school year even though this is my own personal computer?

Yes. The Acceptable Use Policy for CMS remains in effect even when you are using your own computing device such as a laptop, Smartphone, iPad, etc. Violating the terms of the AUP would be a student code of conduct violation.

14. How will theft, loss, or damage of a personally owned device be handled in a school?

The guidelines for the BYOT program specifically address the risk of students bringing their own devices to school. The school is NOT RESPONSIBLE for lost, stolen, or damaged devices.

15. What is the range of the network?

The range of the network will depend on the infrastructure at your school. The priority for connectivity is as follows: Classrooms, Mobiles, Cafeterias, Gyms, Athletic Facilities.

16. I have an app that doesn't seem to be working on the Guest Network?

When accessing the guest network, you must first open up a browser in order to receive the AUP Agreement page. Once that is accepted, you are on the guest network.

17. I need to save my work to the CMS network. Why can't I access this resource?

You are on the CMS Guest Network. It is not the same as the network you would normally access from a school computer. You will not see your home folder, so you will need to save your work in another place. Some options include a flash drive, your own hard drive, or your CMS Gagle account.

18. Will students be able to recharge devices during the school day?

Students are not permitted and should not have the expectation that they will be able to charge devices at school. Many school buildings do not have the capacity to handle additional electrical demands for charging personally owned devices.

19. Will students be able to use ear buds or other types of headsets?

Students may use these during class with the permission of the teacher or administrator.

20. Will students be able to record teachers or classmates (audio or video)?

With the permission of the teacher or administrator, students can make recordings.

21. Can teachers require students to bring their own devices?

No. Students are not required to participate in the BYOT program.

22. Will students be able to use their devices before or after school? During lunch? In the media center?

Access to devices at the school outside of class time will be determined by each school - please refer to your school's BYOT policy on this matter.

23. How will students be able to print?

Students will not have the capability to print from their devices in school.

24. I'm connected to the Guest Network, and I am not receiving my personal email, what should I do?

Since the guest network follows the same filtering policy as other CMS networks, you will not be able to receive personal email while connected to the guest network.

Internet Acceptable Use Policy

Accessibility

The Internet connects computers, computer networks, and individual subscribers around the world. Through the CMS network, students may have access to information and news, some of which may include advertisements, public domain information, and information in university libraries, the Library of Congress, and other research institutions. Students may also create individual web pages and help to create and maintain school web pages.

Restrictions

The CMS network is not a public access service or a public forum. CMS retains the right to place restrictions on material accessed or transmitted by students. CMS employees may access student accounts, e-mail messages, or web pages at any time in order to assure that the system has not been used for inappropriate purposes. Students are directed not to access information that does not have an educational purpose, is obscene, advocates or condones unlawful or dangerous acts, or advocates or condones violence or discrimination towards other people. Further, students should have no expectation of privacy for any information created, transmitted, recorded, stored, or posted on or through the CMS network. Other restrictions on student use are included in the regulations accompanying.

Filters and Monitoring

CMS will use filters that, within the limits of technology, control and screen out information that is inappropriate, obscene, pornographic, or harmful to minors. Further, teachers and other staff will monitor student activity while using the CMS network. However, despite the filtering of information and monitoring by teachers and staff, students might access information that parents consider objectionable. Parents should instruct their child(ren) regarding any additional parental restrictions on information that is allowed to be accessed. However, CMS does not accept responsibility for enforcing restrictions imposed by parents. **It is the responsibility of parents to install parental controls on any PTD their child brings to school to prevent access to information they consider inappropriate.**

Student Acceptable Use Policy

Before students are given access to the Internet from CMS computers or otherwise allowed to use the CMS network, they must accept the terms of the "Student Internet Use Agreement." This Agreement defines the educational objectives and guidelines for use, informs student users that their online activities are subject to monitoring, and sets forth unacceptable uses that may lead to revocation of access and possible legal action. Parents of students younger than age 18 who do not want their children to use the CMS network and/or to access the Internet at school must notify the school in writing.

Disclaimer

CMS is not responsible for theft, loss, or damages to any PTD brought to school, or any injuries suffered as a result of a student's use of the CMS network or a PTD. Students and parents maintain sole responsibility for all PTDs brought to school.

Security

Anyone who becomes aware of suspicious or inappropriate use of data, CMS network or computer system abuse, or breaches of security should alert a teacher or other supervisory staff as soon as possible. Any person who accidentally accesses sites that violate this policy should report such sites to the appropriate teacher or other staff member.