Rutherford County Schools
Bring Your Own Device

Why BYOD (Bring Your Own Device)

Rutherford County Schools is committed to ensuring students are provided an environment which maximizes the integration and use of technology by students and staff as part of their daily educational experience. BYOD allows students additional opportunities to adapt, manage, and participate in a technological world, and helps fulfill the mission statement of our system of empowering today's students to grasp tomorrow's opportunities.

BYOD in Rutherford County

For the 2014-2015 school year, Rutherford County is allowing all 6th – 12th grade students to bring their own technology devices to their school campus to be used for educational experiences and activities. All students and staff are expected to complete the RCS Acceptable Use Policy (AUP) prior to participating in any online activities with either their own device or with school-purchased technology. Students and staff who do not complete an annual AUP will not be allowed to access the technology of Rutherford County Schools or the RCS Wi-Fi network.

Students and staff who connect to RCS Wi-Fi using their personal device are agreeing with the terms with the RCS Wi-Fi Connection Agreement. This agreement states:

> *Rutherford County Schools is providing wireless connectivity for students and staff as an educational resource. Students and staff must utilize the RCS-Secure Wi-Fi network when accessing the internet and sign in using their district usernames and passwords. RCS offers no guarantees of privacy or that information shared can be protected. Use of the RCS-Secure wireless network is entirely at the risk of the user, and RCS is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury, or damages resulting from the use of the wireless connection. Connecting personal devices to the RCS-Secure Wi-Fi indicates you are agreeing to all cautions and policies as they pertain to non-district devices and the use of the internet. Students and staff who do not accept the terms of this agreement and the AUP should not access the RCS-Secure network on their personal devices.*

An RCS Wi-Fi Connectivity Opt-Out form is available for parents and guardians who wish to opt-out of this resource.

Students and staff will access the internet through the RCS-Secure Network, which is available in every building in our district. Students and staff will utilize their RCS usernames and passwords to access the Wi-Fi.

RCS board policy 6.312 outlines the parameters for students wishing to participate with BYOD. Please read this policy carefully for additional information regarding BYOD. For your convenience, it is included in the appendix of this document

Important Information for Students and Parents

- You may begin participating in BYOD once you have completed and turned in your RCS AUP form. The AUP agreement remains in effect even when you are accessing the internet with your own device. Student filtering is a requirement of all schools regardless of the device.
- Students are not required to bring their own devices to school. However, they are still required to complete an AUP agreement to use school technology.
- All students must connect to RCS Wi-Fi by choosing the RCS-Secure network from their device's Wi-Fi settings. You will use the same username and password you use when logging in to a school based computer. Students who have devices with other data plans (AT&T, Verizon, Sprint, T-Mobile, etc.) are still required to utilize the RCS-Secure Wi-Fi network.
- The teacher in the classroom has the final say on procedures in the classroom. If a teacher asks you not to use your device at a particular time, then you must follow those directions.
- Personal devices must remain in silent mode at all times except when it is being used for instructional purposes and permission has been granted by the instructing teacher.
- Individual schools will have various zones where personal devices are and are not allowed. Users are required to follow these procedures on where a device can and cannot be used.
    - Green Zones: Open use of device
    - Blue Zones: Devices are permitted for specific instructional use
    - Yellow Zones: Devices are on silent and out of sight
    - Red Zones: Prohibited
- As stated in board policy 6.312: "Unauthorized use or improper storage of a device will result in confiscation of the device and appropriate disciplinary action." Possession of a personal device under the RCS policy is a privilege which may be forfeited by a student who fails to abide by all policies and procedures. Refer to the attached BYOD User Guidelines document for further guidance.
- The device may not be used to record, transmit, or post photographic images or video of a person, or persons on campus during school activities including district provided transportation unless assigned by the teacher and allowed by the RCS Acceptable Use, Media Release, and Internet Safety Procedures.
- Connectivity and Technical issues that may arise with the device remain the responsibility of the owner of the device. Students and parents should consult their owner's manual or other support resources as needed. Students should test their devices outside of instructional time.

    - Windows devices may require the installation of a configuration file to allow for connectivity. In these cases, students can work with the school's Technology Coach or support staff to address this one-time issue.
- Students should ensure devices are charged prior to bringing them to school each day.
- The focus of classroom time is instruction in the content area. Teachers will not be able to assist students with their devices during this instructional time.
- District firewalls and filters are in place to lessen the risk of outside threats.

Personal Responsibility

As with any personal item you bring from home, there are risks involved when you bring your own device to school. RCS is not responsible for theft or damage done to the device while at school. It is important that students and parents record the device's serial number in the event it comes up missing. A school administrator should be contacted in the event theft occurs so they are aware of the situation.

Important Information for Staff

- Teachers are encouraged to incorporate and leverage student owned devices to assist with instruction in his/her classroom and to integrate these devices into their coursework. The use of personal devices should be driven by the needs of the lesson and be meaningful opportunities for students. Teachers are encouraged to work with their school Technology Coach on ways to fully implement BYOD in their classroom.
- Connectivity and technical issues may arise with student devices during your class. These are not RCS devices, and resources are not allocated at this time to assist with troubleshooting problems. The focus of classroom time is instruction in the content area. Teachers are welcome to help if they choose, but it is not the teacher's responsibility to ensure student owned technology is functioning properly. The school's Technology Coach may be an additional resource. However, they are also limited in time and availability to troubleshoot student computers. Ultimately, students should work with user manual or other supports that came with the device.
- Staff members are also required to complete the RCS AUP agreement at the beginning of each year.
- Staff members are also required to connect to the RCS-Secure Network using their district username and password credentials.
- Students are required to follow the guidelines of the AUP on their personal devices just as they do on school-owned devices. Any disciplinary infractions that occur from using technology tools should be referred to a campus administrator.
- Theft issues should be reported to campus administration. RCS is not responsible for theft or damage done to the device while at school. Please remind students to record the serial number of the device in case theft occurs.

Digital Citizenship

Internet safety is a shared responsibility between the student, parent, and school. It is important for parents to continuously monitor their child's activities online. RCS Technology Coaches in conjunction with guidance counselors, school resource officers, teachers, and other support staff provide internet safety instruction in grades K – 12. Topics covered include:

- Internet Safety/ Keep it Private
- Netiquette
- Cyberbullying
- Online decisions = Offline Consequences

Recommended Devices

RCS does not recommend a specific piece of technology for students to use. Families should consider their specific needs of the needs of the individual student. However, there are some general specifications that can be considered with any device.

The ideal device for school use:

- Is lightweight and sturdy
- Has a protective carrying case
- Has several hours of battery power
- Has wireless capabilities

Appendix

A. RCS Wi-Fi Connection Agreement Opt-Out form
B. BYOD User Guidelines

Additional Information

- RCS Policy 4.406 Use of the Internet
  http://www.boardpolicy.net/documents/detail.asp?iFile=14563&iType=4&iBoard=74

- RCS Policy 6.312 Use of Personal Communication Devices and Cellular Telephones
  http://www.boardpolicy.net/documents/detail.asp?iFile=14673&iType=6&iBoard=74

Rutherford County Schools
BYOD – Wi-Fi Connection Opt-Out Form

Students and staff who connect to RCS Wi-Fi using their personal device are agreeing with the terms with the RCS Wi-Fi Connection Agreement. This agreement states:

> Rutherford County Schools is providing wireless connectivity for students and staff as an educational resource. Students and staff must utilize the RCS-Secure Wi-Fi network when accessing the internet and sign in using their district usernames and passwords. RCS offers no guarantees of privacy of information shared can be protected. Use of the RCS-Secure wireless network is entirely at the risk of the user, and RCS is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury, or damages resulting from the use of the wireless connection. Your signature to this agreement indicates you are agreeing to all cautions and policies as they pertain to non-district devices and the use of the internet. Students and staff who do not accept the terms of this agreement and the AUP will not be able to access the RCS-Secure network on their personal devices.

If you wish to opt out of this resource, please complete the information below. By completing this form you are indicating you do not want your child to be allowed access to the RCS-Secure Wi-Fi network.

Wi-Fi User's Name: _____

Wi-Fi User's Signature: _____

School _____ **Homeroom:** _____

Parent/Guardian's Name: _____

Parent/Guardian's Signature: _____

Rutherford County Schools
BYOD User Guidelines

User must respect and protect the privacy of others by:

1. Using only assigned accounts
2. Only viewing, using, or copying passwords, data, or networks to which they are authorized.
3. Refraining from distributing private information about themselves or others.
4. Refraining from recording, transmitting, or posting photographic images or videos of a person or persons on campus during school activities including district provided transportation unless assigned by a teacher as allowed by the RCS Acceptable Use, Media Release, and Internet Safety Procedures.

Users must respect and protect the integrity, availability, and security of all electronic resources by:

1. Observing all district internet filters and network security practices.
2. Reporting security violations to a teacher or school official.
3. Not destroying or damaging data, networks, or other resources that do not belong to them.

Users must respect and protect the intellectual proper of others by:

1. Following copyright laws (not making illegal copies of music, games, or movies).
2. Citing sources when using others' work.

Users must respect and practice the principals of community by:

1. Communicating only in ways that are kind and respectful.
2. Reporting threatening or discomforting materials to a teacher or administrator.
3. Not intentionally accessing, transmitting, copying, or creating materials that violate the district's Acceptable Usage Policy (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
4. Not intentionally accessing, transmitting, copying, or creating material that is illegal.
5. Refrain from bullying, selling, advertising, or otherwise conducting business.

Adapted from:

"BYOD Toolkit." *K-12 Blueprint*. Intel Education, n.d. Web. 08 July 2014