Personal Device Agreement

Rutland Area Christian School (RACS) teachers and administrators believe that providing network access for personal electronic devices will enhance the educational experience for RACS students by expanding access to the resources provided by the Internet. For this reason, RACS will allow personal devices with these considerations:

1. **Acceptable Devices.** Students may access the RACS network with a mobile personal device (iPod, iPad, iPhone, Android Tablet, Android Phone, Tablet, Smart Phone, Laptop, Net Book, Chrome Book, etc.).

2. **Personal Responsibility.** RACS assumes no responsibility for the loss of, theft of or damage to any personal device that a student connects to the wireless network or any information on that device. Personal electronic devices are brought to school at your own risk. Police reports will NOT be filed by the RACS Police for LOST personal electronic devices. Police reports may be filed for the theft of a personal electronic device with a value greater than $500.00 when there is a suspect, witness or other evidence substantiating that a crime occurred.

3. **Security.** Personal devices shall not impair the security of the RACS network. This expectation includes but is not limited to:

    - Students are expected to maintain up to date antivirus and antispyware protection on all devices that are connected to the RACS wireless network. Devices without up-to-date security programs may be denied access to the network.

    - Students are expected to safeguard all network passwords. Students should not share network passwords with others and should change passwords frequently. Students are expected to notify an administrator immediately if they believe their student account has been compromised.

    - Students are expected to log onto the network using their personal account only. They should not allow others to use their account or use the accounts of others, with or without the account owner's authorization.

4. **No Information Technology (IT) Department Support.** Students are responsible for setting up and maintaining the devices that they connect to the network. RACS will not provide IT support for personal devices.

5. **Authorized Use.** Students may use the network when they are not in class. Students may not use the network in class (including Study Hall) unless authorized by the teacher of that class.

6. **Inappropriate Use.** The RACS network is a shared and limited resource and all users have an obligation to use that resource responsibly. Students are provided access to the RACS network primarily for educational purposes. Incidental personal use or the network is acceptable, but students should not use the network for personal activities that consume significant network bandwidth or for activities that violate school policy or local law. These include but are not limited to:

    a. Online gaming (e.g., Halo) unless approved by a teacher.

b. Peer-to-peer networking. A peer-to-peer network is created when two or more PCs are connected and share resources without going through a server. They can expose computers to worms and viruses.

c. Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights; or if the software, music, or movies are not being used for educational purposes.

d. Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material.
Conducting any activity that is in violation of school policy or local, state or federal law, including using the system to bully others.

e. Participating in political activities.

f. Conducting for-profit business.

g. Using hacking tools on the network or intentionally introducing malicious code into the RACS network.

h. Using any software or proxy service to obscure either the teacher or student's IP address or the sites that the student visits.

i. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.

j. Accessing or attempting to access material or systems on the network that the student is not authorized to access.

7. **No Expectation of Privacy.** The school can and does monitor Internet access and activity on the school's network, including but not limited to sites visited, content viewed and e-mails sent and received. The school may examine a teacher's or student's personal device and search its contents if there is a reason to believe that school policies, regulations, or guidelines regarding access to the network or use of the device have been violated.

8. **Disruptive Activity**. Students should not intentionally interfere with the performance of the wireless network and/or the school's overall network.

9. **Unauthorized Networks**. Students may not create unauthorized wireless networks to access the RACS wireless network. This includes establishing wireless access points, wireless routers and open networks on personal devices.

10. **Consequences of Inappropriate Use.** Students who misuse RACS' network will be subject to discipline which may include loss of access to the network or all Internet access and/or other appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws. RACS staff members who misuse the network are subject to disciplinary or legal action including termination.

11. Student Expectations for Personal Devices.

a. Connecting a personal device to the RACS network provides access to filtered Internet and access to the student portal which allows access to web-based RACS resources. Access to the Internet will be filtered according to school policy.

b. The preferred personal device is a netbook or laptop as they provide the best viewing of instructional content.

c. Students can connect to the RACS network using laptops, netbooks, tablets, smart phones, or PDA's.

d. Students are not allowed to bring a personal desktop computer to school.

e. Each student is responsible for his/her own device: set-up, maintenance, charging and security. Teachers will not store student devices at anytime, nor will any RACS staff member repair or work on a personal device.

f. Gaming, chatting, MySpace, Facebook, etc. are not allowed allowed. Use of device is for educational purposes only and must be approved by the teacher.

g. The teacher establishes the device-use policy for his/her classroom and will monitor the students' access if used in the classroom.

h. Students are expected to abide by guidelines set forth in the Acceptable Use Policy and the Personal Device Agreement. If a student uses a personal device in an inappropriate manner, consequences may be imposed based on the Acceptable Use Policy, the Student Conduct Code and the Personal Device Agreement.

i. Students should not connect a school-provided computer to the RACS wireless network. The RACS wireless network is only for personal devices and will not provide print services or RACS instructional software that is not web-based.

12. Teacher Expectations

a. Teachers will request that the students close the screen while the teacher is talking or keep at 45 degrees (anytime a teacher deems necessary).

b. If the teacher allows device use in the class, the teacher must monitor the student access.

c. It is still the teacher's classroom; if device use is not required students do not have to use them.

d. Devices can be searched by administrators. Report any inappropriate use (office referral).

e. Teachers are expected to circulate around the room and monitor often! The teacher is responsible for monitoring students if he/she allows them to use devices in the classroom.

f. Teachers are expected to do research before planning an online activity. All handheld devices are not created equal.

g. Personal devices used at RACS will fall under the same policies as school-owned devices. Teachers should not store student devices; they are the owner's responsibility at all times.

h. Teachers will not provide to students any charger or power sources belonging to a staff member or any RACS-owned device for use with personal student devices.

Personal Device Agreement
Student/Parent Signature Page
Rutland Area Christian School
2015-2016

We have read the Rutland Area Christian School Personal Device Agreement and will comply with its terms and policies.

My child plans to bring a personal mobile computing device to Rutland Area Christian School to use for educational purposes. We understand that bringing personal devices is at our own risk. We also understand that at anytime our personal device can be examined for its contents and searched if there is a reason to believe that school policies, regulations, or guidelines regarding access to the network or use of the device have been violated.

Student Name (print) _____

Student Signature _____

Parent Signature _____

Phone Number _____

Date _____