**Bring Your Own Device Procedures**

**Introduction**

The St. Johns County School District (SJCSD) is committed to providing students and staff a next generation learning environment in which every student has access to learning experiences and instruction designed around communication, collaboration, creativity, and critical thinking.  Furthermore, the District is committed to immersing our students in the creation of knowledge and empowering our students to discover and innovate.

To expand the integration of technology use in the classroom, the District began a pilot in 2016-17 that promotes the use of student owned mobile devices in school called the BYOD program.

Beginning in the 2017-18 school year, Bring Your Own Device (BYOD) has been expanded to all district schools (except charter and DJJ schools) with emphasis on grades 6-12 that have begun to use Schoology. Schoology is a Learning Management System (LMS) that promotes digital instruction, collaboration and communication between teachers, students and parents.

Participation by students in the BYOD program is **NOT** required.   Personally owned devices are a supplement to the equipment already in use in the classroom.  BYOD is an optional program; parents are not required to purchase a device.  When electronic devices are used to enhance learning in the classroom, students without a personal device will be provided access to an appropriate district-owned device based on availability or provided with an alternative way of completing the activity.

This BYOD policy will allow students, parents, staff and guests to use their own technology during the day when authorized by the teacher to enhance the learning experience.  Examples of the types of technology which can be used are Windows laptops/tablets, Mac laptops, and iPads.  Recommended mobile device specifications for parents to reference are posted on the District’s BYOD web site.

It is one of the technology goals of the district to ensure that each User’s interactions with technology contribute positively to the learning environment both at school and in the community.  SJCSD also recognizes that Users have widespread access to both technology and the Internet; therefore, use of personal devices and connectivity is considered to be included in the Acceptable Use Policy (AUP).

All rules and policies applicable to the use of district owned technology and the AUP, apply to student-owned devices (BYOD) as well.

**Student Supervision and Security**

SJCSD does provide content filtering controls for student access to the Internet using SJCSD’s network as well as reasonable adult supervision, but at times inappropriate, objectionable, and/or offensive material may circumvent the filter as well as the supervision and be viewed by students.  Students are to report the occurrence to their teacher or the nearest supervisor.  Students will be held accountable for any deliberate attempt to circumvent SJCSD technology security and supervision.

Students using mobile and cellular devices while at school, during school or district-sponsored activities are subject to the terms and conditions outlined in this document and are accountable for their use.

**Terms and Conditions**

Access to the SJCSD network by student owned devices will be in the form of a wireless connection.  This wireless access provided to the devices is designed to enhance the students’ educational experience and outcomes.  Connecting to the SJCSD Wi-Fi network with personal devices is a privilege, not a right.  Permission to bring and use privately owned devices is contingent upon adherence to SJCSD guidelines (including the AUP).  If a privately owned device is used by a student to disrupt the educational environment, in the sole opinion of SJCSD, that student’s privileges may be limited or revoked.

SJCSD reserves the right to take immediate action regarding activities:

1) that create security and/or safety issues for the SJCSD network, Users, schools, network or computer resources;  
2) that expend SJCSD resources on content it determines lacks legitimate educational content/purpose; or  
3) other activities as determined by SJCSD as inappropriate.

These Terms and Conditions apply to all devices on the network including student-owned (BYOD).

Here are examples of inappropriate activity on the SJCSD network:

1. Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Obtaining and/or using anonymous email sites, spamming, spreading viruses.
4. Causing harm to others or damage to their property.
5. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
6. Deleting, copying, modifying, or forging other Users’ names, emails, files or data, disguising one’s identity, impersonating other users, or sending anonymous email.
7. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs.
8. Using any SJCSD computer/mobile devices to pursue “hacking,” internal or external to SJCSD, or attempting to access information protected by privacy laws.
9. Accessing, transmitting or downloading large files, including “chain letters” or any type of “pyramid schemes.”
10. Using web sites, email, networks, or other technology for political uses or personal gain.
11. Users must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
12. Users must adhere to all copyright laws.
13. Users are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.

**BYOD Guidelines**

1. Students may use a privately owned electronic “Internet ready” device on the SJCSD wireless network with teacher or administrator permission.  
   –
2. The use of a privately owned electronic device is to support and enhance instructional activities.  
   –
3. Students are not to share passwords and keep personal information private.  
   –
4. No privately owned electronic device may be connected to the SJCSD network by a network cable plugged into a data outlet. Network access is provided via Wi-Fi access only.  
   –
5. No student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds. This includes, but is not limited to using a privately owned electronic device as a cabled or wireless hotspot.  
   –
6. Voice, video and image capture applications may only be used with teacher or administrator permission.  
   –
7. Sound should be muted unless the teacher or administrator grants permission for use of sound associated with the instructional activities. A teacher or administrator may permit the use of ear buds or other types of headphones.  
   –
8. The privately owned electronic device owner is the only person allowed to use the device.  
   –
9. No student shall use any computer or device to illegally collect any electronic data or disrupt networking services.  
   –
10. Devices are brought to school at the students’ and parents’ own risk. In the event that a privately owned device is lost, stolen or damaged, SJCSD is not responsible for any financial or data loss.  
    –
11. Violation of school policies, school board policies or regulations, local, state and/or federal laws while using a personal electronic device on the SJCSD wireless network will result in appropriate disciplinary and/or legal action as specified in the *Student Handbook* and *Code of Student Conduct*, School Board policy and regulation as well as by local, state and/or federal law.  
    –
12. School or District personnel are not permitted to repair, correct, configure or troubleshoot personal devices or software.  
    –
13. The School District reserves the right to take a privately owned electronic device that is being used or suspected of being used in violation of these Guidelines, the Code of Student Conduct, School Board policy or regulation, or local, state, or federal law or regulation.  
    –
14. The School District may search privately owned electronic devices when reasonable, articulable suspicion exists that the device was used in violation of these Guidelines, the Code of Student Conduct, School Board policy or regulation, or local, state or federal law or regulation. Such searches are limited to the scope of suspected violation.  The School District may contact appropriate law enforcement agencies and provide information concerning the use of the device for suspected violations of law or regulations.