SSSD Bring Your Own Device Policy Structure

1. Student Device Overview
   1.1. Striving to achieve the most up-to-date, seamless, and effective 21st Century learning environment, the Shanksville-Stonycreek School District is piloting a program that will change the landscape of technology education at the district. Students and staff will have the opportunity and ability to use their own personal computing device (laptop, netbook, tablet, smartphone, etc.) during the course of the school day for educational purposes. Students will (with instructor permission) use their own device to have access to the Internet and the SSSD cloud network, be able to collaborate with other students, and use device specific applications. The impetus of this initiative is for students to use their own device, which they are comfortable with and use effectively to further streamline their education. This in turn will morph the focus of technology in education from learning the assigned classroom device to authentic student learning. The following policies will be put in place to maintain the district’s level of network security, educational integrity, and student success. However, inasmuch as this is a “ready, shoot, aim” movement, additional policies will need to be added and existing policies altered or eliminated.

   1.2. The Shanksville-Stonycreek School District looks to implement this program in the spring semester of the 2011-2012 school year. The district will pilot the program with the sophomore class, and with a degree of success implement the program throughout the high school in the 2012-2013 school year.

   1.3. All users of personal computing devices should be aware that use of their device is a privilege and not a right. This privilege can be revoked for misuse or the entire initiative can be cancelled due to network abuse.

2. Acceptable Devices
   2.1. Student computing devices shall be defined as any device that achieves an Internet connection and can be used in an educational capacity to create content, collaborate with peers and experts, or positively enhance classroom instruction.

   2.2. Acceptable devices include but are not limited to the following:
   2.2.1. laptop - portable computers to be used in different environments
   2.2.2. netbook – a smaller form factor device than a laptop
   2.2.3. tablet - a portable computer that uses a touchscreen as its primary input device
   2.2.4. ereader - a portable hardware device designed for reading digital publications
   2.2.5. iPod - portable music player with Internet access and file system capability
   2.2.6. smartphone - mobile phone that includes advanced functionality beyond making phone calls and sending text messages

   2.3. Unacceptable devices will be defined as any device that is primarily used for gaming such as DS, DSI, etc.

   2.4. Devices will be deemed acceptable or unacceptable on an individual basis by SSSD administration.
2.5. Students or staff wishing to use a device must complete a “registration process” for the device with school officials and obtain a “license” for the device. Multiple devices will require multiple licenses. Upon successful registration the device can then connect to the SSSD network as outlined in section 3.

3. Achieving Network Connection

3.1. For the purposes of this initiative, the SSSD network is synonymous with the current “Student” SSID, which grants users access to Internet resources, but does not allow access to the internal district network. The SSSD network is filtered through the Sonic Wall Web filtering service and all policies regarding bypassing the filter remain constant with the district’s current policy on misuse of technology (also outlined in section 4).

3.2. Upon successful completion of the device registration process, users will then have access to the SSSD network. The connection process requires the following steps:

3.2.1. Device is connected to SSSD student network using generic password

3.2.2. Upon executing Internet access, the user will be directed to a Web page where a unique login is necessary to access the Internet

3.2.3. User will achieve monitored access to all Internet resources, though Sonic Wall filters still will be in effect

3.2.4. All users will be issued an account in the SSSD cloud, where they have reign to create, save, and collaborate

4. Use of Device/Collateral Use

4.1. Use of personal devices on the district network is intended to enhance, streamline, and personalize educational experiences and opportunities within the district. All users of personal devices do so with the understanding that personal devices are to be primarily used for educational endeavors. However, some personal use of devices may be acceptable under cooperation with the district.

4.2. Within the classroom setting, students are to use their personal device solely for educational purposes as directed by the classroom instructor. Examples of appropriate use are:

4.2.1. research on Internet

4.2.2. collaboration with peers/experts

4.2.3. use of the SSSD cloud

4.2.4. use of subject specific software

4.2.5. any other use deemed acceptable by the instructor

4.3. Students should not use personal devices for engaging in activities not consistent with instructor’s guidelines for that particular lesson or course. Examples of such activities are:

4.3.1. random browsing of Internet

4.3.2. any and all texting

4.3.3. photographing or audio/video recording events within the classroom (without permission of teacher and consent of all involved)

4.3.4. playing games

4.3.5. listening to music/watching videos

4.3.6. streaming/download content

4.3.7. bypassing of district filtering
4.4. Students who misuse or inappropriately use their device during instructional time will be subject to the following discipline structure (level of discipline is at the discretion of SSSD administration):

4.4.1. 1st offense – warning (depending on severity)
4.4.2. 2nd offense – loss of privilege of device for 1 week
4.4.3. 3rd offense – loss of privilege of device for 60 days
4.4.4. 4th offense – permanent loss of privilege of device

4.4.5. In addition to the loss of device privilege, students could also lose all computing and network access depending on the severity of the offense

4.5. All devices in use can have access to the network restricted or eliminated by the district at any time due to misuse or for maintenance.

4.6. Students and staff who use device in an appropriate and constructive manner will be afforded the following allowances:

4.6.1. Students may use device at their discretion during morning cafeteria hours
4.6.2. Students may use their device between class periods, so long as tardiness does not become a persistent issue
4.6.3. Students may use their device during scheduled lunch periods

4.7. Students shall not be permitted to use their device during the following events/activities:

4.7.1. Students may not use their device during morning ceremonies and announcements
4.7.2. Students may not use their device during assemblies and/or meetings
4.7.3. Students may not use their device during study hall unless the activity is educationally based at the discretion of the study hall supervisor.

4.8. Misuse of personal computing devices can and will result in disciplinary action taken against the user with the ultimate consequence being revocation of device use privileges and all computing privileges within the district.

4.8.1. Misuse of personal computing device shall be defined as any activity that

4.8.1.1. inhibits the student’s learning environment
4.8.1.2. inhibits the learning environment of other students
4.8.1.3. causes disruption in the classroom
4.8.1.4. creates a threat to the integrity of the SSSD network and all data, services, applications, and equipment contained within the network
4.8.1.5. creates an unethical educational environment (cheating, plagiarism, etc.). In this situation, the guidelines and procedures contained in the Blue & Gold Handbook will be followed

4.8.2. Personal devices that are suspected of having inappropriate, illicit, unethical, incriminating, or damaging content contained within are subject to search and seizure as is protocol with student backpacks, lockers, or any other materials. Failure to submit device for inspection will result in permanent revocation of device privileges.

5. Service/Maintenance

5.1. Inasmuch as the personal computing device is the property of the individual student/staff, responsibility for maintenance and service for the device falls upon the owner of the device and not the Shanks ville-Stonycreek School District. All preventive and routine maintenance and
required and emergency service will be administered by the owner of the device or third party designated by the owner. These services include but are not limited to:

5.1.1. operating system updates
5.1.2. software installation
5.1.3. hardware installation
5.1.4. repairs
5.1.5. virus/malware scans or removal

5.2. Personal computing devices will need to be charged at the discretion of the user. Classroom time is not to be used for the re-charging of devices. Assignments or projects incomplete or not accessible due to the malfunction of the device will be considered late or incomplete at the instructor’s discretion.

6. District Software/Resources
6.1. All computing devices owned and used by students or staff will not be equipped with any district software or applications. Users will be responsible for procuring and installing all software or applications on their respective devices. Likewise, district personnel will not be responsible for instructing the students on use of their device and software or applications installed on their devices. All users are expected to manage their own device from out-of-the-box through end use.

6.2. The district will establish an SSSD cloud network where users will have access to storage space and free, open source software applications such as productivity software. Therefore, the students will not necessarily need access to the district network and will have free software options compatible with industry standard products.

6.3. Classroom instructors will allow students to use the software or application of their choice to complete projects as opposed to using district mandated software. However, any software used must be approved and compatible with that the instructor uses to evaluate student products.

7. Security (Content & Hardware)
7.1. All content contained on any personal computing device to be used on the SSSD network is to be school appropriate in nature and in no way harmful to the district network. The district has the right to search a device or revoke network access (as detailed in section 4.8) if it is determined the device is a detriment to the network, the learning process, or the student. Examples of detrimental materials include, but are not limited to:

7.1.1. virus
7.1.2. malware
7.1.3. illicit downloading
7.1.4. streaming media
7.1.5. inappropriate materials

7.2. Personal computing devices are the property of the owner, not the district. Students or staff are responsible for the safety and well-being of their personal device. The district will not be held liable for any damage, vandalism, or theft of any device brought into the district. The district will handle any incidents in accordance with guidelines in place for any personal property of students or staff.
7.3. Any persons committing vandalism to or theft of a device will face consequences as outlined in the district handbook.