# BYOD & 1:1
# Acceptable Use Policy

## Definitions

- **User** includes anyone, including employees, students, and guests, using SSD technology, including, but not limited to, computers, networks, Internet, email, chat rooms and other forms of technology services and products.

- **Network** is wired and wireless technology networks including school and district networks, cellular networks, commercial, community or home-based wireless networks accessible to students.

- **Equipment** are cellular phones, MP3 players, iPod, and portable computers such as laptops, iPads, desktops, tablets and netbooks, as well as portable storage devices.

Technology provides students with unique and powerful ways to enhance their learning. Stewartville School District (SSD) supports the use of technology for the purpose of enhancing and supporting learning and is pleased to offer Users access to computer networks so that they can access district-supplied technology to enhance learning any time of day.

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. Negative use of technology through SSD-owned devices inside or outside of our schools that degrades or defames other Users, or members of our community is unacceptable. SSD 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 this Acceptable Use Policy (AUP).

Access to SSD's network is a privilege, not a right. The use of technology whether owned by SSD or devices supplied by the Users entails personal responsibility. It is expected that Users will comply with SSD rules, act in a responsible manner, and will honor the terms and conditions set by the classroom teacher, the school, and SSD. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary. In particular, students will be held accountable for their actions and are encouraged to report any accidental use immediately to their teacher or school administration.

With the increased usage of free educational applications on the Internet, digital storage areas containing sensitive User information, may or may not be located on property of the school. In some cases, data will not be stored on local servers. Therefore, Users should not expect that files and communication are private. SSD reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of SSD property, network and/or Internet access or files, including email.

SSD has a private and secure system for sensitive school records, which will be managed by SSD Information Technology Staff.

# Google Apps in Educational Applications

SSD is offering Users a free educational suite of applications for use to enhance teaching and learning.Google Apps is a concept known as "cloud computing" where services and storage are provided over the Internet. SSD is providing Users Google Message Security. This service provides System Administrators the capability to limit messages based on where they are from, where they are going, or the content they contain. SSD will use this technology protection measure to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network.

In order for Users to gain access to Gmail and his/her Educational Google Applications account on the Internet, SSD must obtain parental permission for a minor under the age of 14 years. Students 14 years and older are also required to acknowledge and accept SSD's terms and conditions prior to obtaining access to technology within our schools. Under both circumstances, this may be accomplished by completing an AUP and any other necessary permission forms. More information can be found at https://policies.google.com/?hl=en.

# Schoology

SSD is offering users a free learning management system (LMS) called Schoology. Schoology is a cloud based LMS where services and storage are provided over the Internet. The platform provides a full suite of learning management tools. Students, teachers and parents can access Schoology.com through the school district's Enterprise account.

In order for Users to gain access to Schoology, SSD must obtain parental permission for a minor under the age of 14 years. Students 14 years and older are also required to acknowledge and accept SSD's terms and conditions prior to obtaining access to technology within our schools. Under both circumstances, this may be accomplished by completing an AUP and any other necessary permission forms. More information can be found at https://www.schoology.com/privacy.

# Terms and Conditions

These are examples of inappropriate activity on the SSD network, but SSD reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the SSD network, Users, schools, network or computer resources; 2) that expend SSD resources on content it determines lacks legitimate educational content/purpose; or 3) other activities as determined by SSD as inappropriate.

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. Selling or purchasing illegal items or substances.

4. Obtaining and/or using anonymous email sites, spamming, spreading viruses.

5. Causing harm to others or damage to their property.

6. 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.

7. Deleting, copying, modifying, or forging other Users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.

8. 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, or disrupting any computer system performance.

9. Using any SSD computer/mobile devices to pursue "hacking," internal or external to SSD, or attempting to access information protected by privacy laws.

10. Accessing, transmitting or downloading large files without prior permission.

11. Using web sites, email, networks, or other technology for political uses or personal gain.

12. SSD internet and intranet property must not be used for personal benefit.

13. 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.

14. Advertising, promoting non-SSD sites or commercial efforts and events

15. Users must adhere to all copyright laws.

16. 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.

17. Student takes full responsibility for his or her laptop and keeps it with himself or herself at all times. The school is not responsible for the security of the laptop.

18. Student understands that any software needed for educational use or for the use to access the districts network will be installed on their device.

19. May not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging).

20. Student complies with teachers' request to shut down the computer or close the screen.

21. Student acknowledges that the school's network filters will be applied to one's connection to the internet and will not attempt to bypass them.

22. Student understands that bringing on premises or infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of the AUP policy and will result in disciplinary actions.

23. The school district has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.

24. Student realizes that printing from personal laptops will not be possible at school.

25. Laptop is charged prior to bringing it to school and runs off its own battery while at school.

26. Students shall not, at any time, activate any type of wireless networking capability (i.e. hotspots) while on school premises. Only school supplied access to the Internet is allowed at any time or in any facility owned by SSD.

# Cybersafety and Cyberbullying

- **All Users**

Despite every effort for supervision and filtering, all Users and Students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every User must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every User must report security or network problems to a teacher, administrator, or system administrator.

- **Personal Safety**

In using the network and Internet, Users should not reveal personal information such as home address or telephone number.

- **Confidentiality of User Information**

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.

- **Active Restriction Measures**

SSD will utilize filtering software or other technologies to prevent Users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. Attempts to circumvent or 'get around' the content filter are strictly prohibited, and will be considered a violation of this policy. SSD will also monitor the online activities of Users through direct observation and/or other technological means.

# Interactive Web Tools

Technology provides an abundance of opportunities for Users to utilize interactive tools and sites on public websites that benefit learning, communication, and social interaction.

Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school(s). From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge are legitimate and safe. As the site is "public" and the teacher, school, and SSD is not in control of it, all Users must use their discretion when accessing information, storing, and displaying work on the site. All terms and conditions provisions in this AUP also apply to User-owned devices utilizing the SSD network.

# Student Use of Interactive Web Tools

Online communication is critical to the students' learning of 21st Century skills, and tools such as blogs, podcasts, email, social media and chat offer an authentic, real-world vehicle for student expression. Student safety is the primary responsibility of teachers.

Therefore, teachers need to ensure the use of Google Documents, SSD Schoology, classroom blogs, student e-mail, podcast projects, or other Web interactive tools follow all established Internet safety guidelines including:

- The use of Docs, SSD Schoology, blogs, podcasts, social media or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also

inappropriate in all uses of these tools. This includes—but is not limited to—profanity, racist, sexist, or discriminatory remarks.

- Students using Docs, SSD Schoology, blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
- Students should NEVER post personal information on the web (including, but not limited to, last names, personal details such as address or phone numbers, or photographs).
- Students should NEVER, under any circumstances, agree to meet someone they have met over the Internet.
- Students should never link to web sites from their blog or blog comments without reading the entire article to make sure it is appropriate for a school setting.
- Students using such tools agree to not share their username or password with anyone besides their teachers and parents and treat Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

## Student Use of Devices

- SSD has provided some students with technology for use both in school as well as away from school. The SSD-owned devices follow the stipulations outlined in this AUP.
- School Administration and SSD Technology staff may search the student's device if they feel school rules have been violated, which may include, but are not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc.
- Students may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos while at school or during school or district-sponsored activities unless they have permission from both a staff member and those whom they are recording.
- These rules apply to student-owned devices as well. A student-owned mobile device is a non-district supplied device used while at school or during school or district-sponsored activities.

## Student Supervision and Security

SSD does provide content filtering controls for student access to the Internet using SSD'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 SSD 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.

## Deactivating Student Accounts

During a student's enrollment, all of their accounts (Google, Schoology, IXL, etc.) will remain active. When a

student is no longer enrolled via withdrawal, transfer or for any other reason; their account will become inactive and no longer accessible. Upon graduating from SHS, a graduate's account will become inactive on July 1st of their grad year.

# INTERNET USE AGREEMENT–STUDENT

**STUDENT**

I have read and do understand the school district policies relating to safety and acceptable use of the school district computer system and the Internet and agree to abide by them. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print): _____

User Signature: _____

Date: _____

**PARENT OR GUARDIAN**

As the parent or guardian of this student, I have read the school district policies relating to safety and acceptable use of the school district computer system and the Internet. I understand that this access is designed for educational purposes. The school district has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the school district to restrict access to all controversial materials and I will not hold the school district or its employees or agents responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Parent or Guardian's Name (please print): _____

Parent or Guardian's Signature: _____