ACCEPTABLE USE POLICY FOR STUDENTS
STRASBURG-FRANKLIN LOCAL SCHOOL DISTRICT

Please read this Acceptable Use Policy ("Policy") carefully before signing. This Policy is a legally binding agreement. The details of this Policy reflect the Policy of the Strasburg-Franklin Local School District Board of Education ("Board" or "School District").

The Board recognizes that an effective educational system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the School District will use technology resources as a powerful and compelling means for students to learn core subjects and apply skills in relevant and rigorous ways. It is the Board's goal to provide students with rich and ample opportunities to use technology for important purposes just as individuals in workplaces and other real-life settings. The School District's technology resources will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision. The Board will also have procedures or guidelines that provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA. While the Board takes all reasonable efforts to block access to objectionable material, it makes no guarantees about blocking access to such information.

The procedures or guidelines will be designed to:

- Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;

- Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

- Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;

- Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and

- Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA.

Students will receive education about appropriate on-line behavior, pursuant to state and/or federal law.

Parents should be aware that:

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take personal responsibility for his or her use of the network and Internet and avoid objectionable sites.

- Users/parents/guardians are advised that use of any network may include the potential for accessing web sites with inappropriate materials. It is the responsibility of all users to attempt to avoid these sites through prudent use of the Internet. If a student accidentally accesses one of these sites, they should immediately exit from that site and/or notify a staff member.

- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited, whether the attempt is made with district-owned equipment or a personal technological device. The attempts include use of proxies, https, special ports, third party applications, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.

- The Board is not responsible for students accessing information from personal mobile devices using network access outside of the School District network.

I. Personal Responsibility

By signing this Policy, you are agreeing not only to follow the rules stated herein, but are agreeing to report any misuse of the network to a teacher or building principal. Misuse means any violation of this policy, Board of Education Policy, or any other use that is not included in the policy, but has the effect of harming another person or his or her property.

II. Terms of Permitted Use

As used in this Policy, "Network" refers to interconnected computer systems, computer equipment, computer programs, the Internet, electronic mail, IP- or Internet-based telephone systems, and related communication technologies.

A student who submits to the school, as directed, a properly signed Policy and abides by the Policy will be provided computer Network and Internet access during the course of the school year. Students will be asked to sign a new Policy when they enter a new building before they are given an access account. (ex. Elementary to Junior High or Freshman to High School)

By signing the Policy, the students acknowledges and understands the following regarding the use of the computer/network:

1. Computer use is not private. System managers have access to all information and messages, including illegal activities and activities not in the best interest of the School District. Inappropriate and illegal activities may be reported to the authorities as necessary.
2. All electronic data that passes through a District-owned computer or a personally owned device on the School District's network is subject to monitoring and seizure and may be handed over to law enforcement officers.
3. All electronic data created for administrative or instructional purposes under the Board approved curriculum for a course or program is the property of the School District.
4. The rules and regulations of online etiquette are subject to change by the Administration. The student code of conduct is applicable in the online environment and computer Network.
5. The User in whose name a computer account is issued is responsible for its proper use at all times. Users must log off the computer to conclude a session or lock the computer if stepping away. Users retain responsibility for the activity of anyone accessing the computer and/or network under their account. Users shall keep personal account information and all other sensitive information private. Users shall use this system only under the login and password information issued to them, by the School District. Users shall not grant others access to a computer and/or the Network under their login and password.
6. Computer systems and the School District network shall be used only for purposes related to education and shall not be used for personal use.
7. Violation of this Policy could result in the cancellation of user Network privileges and possible discipline under the student code of conduct.

III. Acceptable Use

The School District is providing access to its Network and the Internet for educational purposes *only*. If you have doubt about whether a contemplated activity is educational, you should ask your teacher or building principal if a specific use is appropriate.

IV. Unacceptable Use

Among the uses that are considered unacceptable and which constitute a violation of this Policy are the following:

1. Violating or encouraging others to violate this Policy, the law or Board Policy.
2. Revealing private information about yourself or others. Private information includes, but is not limited to a person's password, social security number, credit card number or other confidential information that has the potential to harm you or others or violate the law if shared with other persons.
3. Uses that cause harm to others or that cause damage to their property.
4. Uses that constitute defamation (i.e. harming another's reputation by lies), or that harass, threaten or bully others.
5. Using profanity, obscenity or other language, which may be offensive to other users.

6. Uses that are for commercial transactions (i.e. buying or selling or making arrangements to buy or sell over the Internet).

7. Use that causes disruption to the use of the computer and/or Network by others or that disrupts the educational process of the School District.

8. Using the system to encourage the use of, or to facilitate the sale of, drugs, alcohol or tobacco.

9. Viewing, downloading or transmitting material that is threatening, pornographic, obscene, disruptive or sexually explicit or that could be construed as harassment or disparagement of others based on their race, national origin, citizenship status, gender, sexual orientation, age, disability, religion or political beliefs.

10. Copying or placing copyrighted material or software on the system without the author's permission and/or in violation of law.

11. Reading, deleting, copying or modifying other User's email or files without their permission or attempting to interfere with another User's ability to use technology resources.

12. Using another person's password or some other identifier that misleads recipients into believing someone other than you is communicating or accessing the Network or Internet.

13. "Hacking," gaining, or attempting to gain unauthorized access to computers, servers, computer systems, internal networks, or external networks.

14. Use that causes excessive consumption of paper and other relevant supplies.

15. Downloading and/or installing freeware or shareware programs without the approval of the Technology Department. This includes use of peer-to-peer file sharing programs.

16. Uploading or otherwise placing or inviting a worm, virus or other harmful form of programming onto the Network or Internet.

17. Plagiarizing copyrighted or non-copyrighted materials for personal gain, recognition, or as graded work.

18. Using social network sites such as Facebook, Twitter, and others and/or forum sites and/or blog sites for the purpose of posting slanderous or otherwise harmful information, whether true or untrue, about the character and/or actions of students or staff.

19. Using instant messaging, text messaging, video messaging and Internet telephone services without the consent of your teacher, supervisor, or director.

20. Uses that degrade or disrupt the operation of the Network or that waste limited computer, paper or telephone resources or cause unnecessary traffic. For example, toner and paper in printers are a cost to the District and must not be wasted. Chain letters and similar multiply forwarded messages are prohibited because, even for non-commercial or apparently "harmless" purposes, they use up limited Network capacity resources. The sending of messages to more persons than is necessary is a misuse of system resources and User time. Large group mailings, such as "all district" or "all building" are reserved for administrative use, subject to any exceptions which may be developed by the Administration or the System Administrator. Unless approval has been granted, you may not send e-mails to more than ten (10) recipients in a single message, subject to exceptions developed by the Administration or the System Administrator. The System

Administrator may also develop specific limitations on the use of graphics, the size, number, and type of attachments, and the overall size of e-mail messages sent on the system. The use of multiple messages, non-system addresses, or other techniques to circumvent these limitations is strictly prohibited.

21. Any use of the Network or a District-issued device that would otherwise constitute a violation of the student code of conduct.

V. Privacy

Network and Internet access is provided as a tool for your education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer Network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials, regardless of storage location.

VI. Vandalism

Vandalism will result in disciplinary action that may include cancellation of privileges, suspension/expulsion and/or prosecution. Vandalism is defined as any malicious attempt to harm or destroy data of another user or equipment or any network connected to any of the Internet backbones. This includes, but is not limited to, the uploading or creation of computer viruses or spyware, erasing, deleting, or otherwise making the school's programs or networks unusable and includes theft or the damaging or defacing of equipment. The School District may hold users (or their legal guardian) personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs incurred, and any costs incurred to return such services to their normal state.

VII. Warranties/Indemnification

The School District makes no warranties of any kind, either express or implied, in the connection with its provision of access to and use of its computer Networks and the Internet provided under this Policy. Neither the Board nor its employees shall be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy and Agreement. The User takes full responsibility of his or her usage and agrees to indemnify and hold harmless the School District and its Board members, administrators, teachers, and staff from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The User and, if the User is a minor, the user's parent(s) or guardian(s) agree to cooperate with the School District in the event of the initiation of an investigation into a user's use or his or her access to its computer network and Internet, whether that use is on a District-issued device or on another device outside the School District's Network.

Acceptable Use Agreement

I agree to follow the Policy as stated herein, and the Board's Policy on Acceptable Use of the School District Network. Should I commit any violation or in any way misuse my access to the School District's computers, computer network, and/or Internet, I understand and agree that my access privileges may be revoked and disciplinary action may be taken against me as outlined in the applicable student code of conduct. I understand that I may exercise my due process rights as provided in the student code of conduct should discipline result under this Policy.

(Please Print Clearly)

Student Name _____ Home Phone: _____

Student ID# _____

Student Signature _____ Date: _____

Parent/Guardian As the parent or legal guardian of the above student, I have read, understand, and agree that my child or ward shall comply with the terms of the _____ School District's Acceptable Use Policy and Board Policy governing access to the district's computers, computer network, and Internet. I understand that access is being provided for educational purposes. I also understand that it is impossible for the School District to restrict access to all offensive and controversial materials. I understand that it is the responsibility of my child or ward to abide by these Policies. I understand that I may exercise my child's due process rights as provided in the student code of conduct should discipline result under this Policy.

(Please Print Clearly)

Parent/Guardian Name _____ Phone _____

Signature _____ Date _____