STUDENT INTERNET/SOFTWARE ACCEPTABLE USE AGREEMENT

1.0 PURPOSE

1.1 The principal or designee shall oversee the maintenance of each school's technological resources and may establish guidelines and limits on their use. It is the student's personal responsibility to educate one's self on the proper and appropriate use of technology in addition to understanding the guidelines within.

2.0 GUIDELINES

2.1 Educational Purpose

The District Internet system has been established for limited educational purposes. This means that students may use the system for classroom activities, professional or career development, and high-quality, educationally enriching research.

Use of the District's computing resources is a privilege, not a right. The District may place reasonable restrictions on the material students can access or post through the system, and may revoke access to these resources if there is a violation of the law or this regulation. Violations of the law or this regulation may also be addressed through the District's Student Conduct and Anti-bullying Policy.

Students may not use the District Internet system for commercial purposes. This means the student may not offer, provide, or purchase products or services through the District Internet system.

2.2 Access to Online Materials

The material students may access through the District's Internet system should be for class assignments or educational research related to a subject or course of study. Use for entertainment purposes, such as personal blogging, instant messaging, on-line shopping, or gaming is not allowed, with the exception of private, District approved bulletin boards, blogs, or chat groups that are created by teachers for specific instructional purposes.

- Students will not use the District Internet system to access, publish, send, or receive any material in violation of applicable law. This includes, but is not limited to: material that is obscene; child pornography; material that depicts, or describes in an offensive way, violence, nudity, sex, death, or bodily functions; material that has been designated for adults only; material that promotes or advocates illegal activities; material that promotes the use of alcohol or tobacco or weapons; material that advocates participation in hate groups or other potentially dangerous groups;

STUDENT USE OF TECHNOLOGY (continued)

materials that promote illegal behavior; material protected as a trade secret or material that can be construed as harassment or disparagement of others based on their race/ethnicity, gender, sexual orientation, age disability, religion, or political beliefs.

- Students who mistakenly access inappropriate information must immediately report such access to a teacher or school administrator. Timely reporting of this material may help to protect a student against a claim that one has intentionally violated this regulation.

2.3 Safety Requirements

To protect one's personal contact information, students shall not share online their full name or information that would allow an individual to locate a student, including family name, home address or location, work address or location, or phone number. Students will not disclose names, personal contact information, or any other private or personal information about other students. If personal information is shared, students will promptly disclose this to their teacher or other school administrator. Any message one receives that is inappropriate or makes them feel uncomfortable should be reported as well. Students should not delete such messages until instructed to do so by a school staff member.

2.4 Unlawful, Unauthorized, and Inappropriate Uses and Activities

The following activities are unlawful, unauthorized, and inappropriate:

- Attempting to gain unauthorized access to the District Internet system or to any other computer system through the District Internet system or go beyond your authorized access. This includes attempting to log in through another person's account or to access another person's files.

- Students will not connect any personal devices to the District network without express permission from the District's Technology Department, unless connected to a District Guest Network. Guest access to the District's open wireless network is provided as a service to the community and is subject to all policies and guidelines covered in the Student Internet/Software Acceptable Use Agreement. This includes, but is not limited to Smart Phones, eReaders, MP3 Players and Personal Computing Devices.

- Making deliberate attempts to disrupt the District Internet system or any other computer system or destroy data by spreading computer viruses or by any other means.

STUDENT USE OF TECHNOLOGY (continued)

- Using the District Internet system to engage in any other unlawful act, including arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, or threatening the safety of any person.

- Attempting to alter or interfere with other users' abilities to post, send, receive, or submit material.

- Attempting to delete, copy, or modify another users' work or identity.

- Creating an unauthorized personal network or "hot spot" in order to gain access to the District Internet is forbidden.

2.5 Inappropriate Language

Students must avoid inappropriate language in their electronic communications. Students will not:

- Use obscene, profane, lewd, vulgar, inflammatory or threatening language or images including but not limited to "sexting"

- Post information that may cause damage or a danger of disruption to your school or any other organization(s) or person(s) without written consent of administration/designee.

- Post photographs, video, or voice recordings of any person(s) of minor age without the consent of administration/designee or the written consent of any adult(s).

- Engage in personal attacks, including prejudicial or discriminatory attacks.

- Harass or bully another person. Cyberbullying is prohibited by state law and district policy.

- Knowingly or recklessly post false or defamatory information about a person or organization.

Students will promptly disclose to a teacher or another school employee any message they receive from any other student that is in violation of the restrictions on inappropriate language.

STUDENT USE OF TECHNOLOGY (continued)

2.6 Plagiarism and Copyright Infringement

Students will not plagiarize works that they find on the Internet. The definition of plagiarism is taking the ideas or writings of others and presenting them as if they were your own.

Students will respect the rights of copyright owners in their use of materials found on, disseminated through, or posted to the Internet. Copyright infringement occurs when students inappropriately reproduce or share a work that is protected by a copyright. Students may not quote extensively from any source without proper attribution and permission. Students may not make or share copies of copyrighted songs or albums, digital images, movies or other artistic works. Unlawful peer-to-peer network file-sharing may be a criminal offense.

2.7 System Security and Resource Limits

Security on computer systems is a high priority. Students are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should students provide their password to another person. Students will immediately notify a teacher or other staff member if they have identified a possible security problem.

If students identify a security problem, they should notify the teacher or other staff member at once. Students should never demonstrate the problem to others.

Students will not download large files unless absolutely necessary. Students will not misuse district, school, or personal distribution lists or discussion groups for sending irrelevant messages.

2.8 No Reasonable Expectation of Privacy

Students should not expect privacy in the contents of their personal files on the District Internet system and records of their online activity. The District's monitoring of Internet usage can reveal all activities students engage in using the District Internet system.

Maintenance and monitoring of the District Internet system may lead to discovery that students have violated this regulation, the student conduct policy, or the law. An individual search will be conducted if there is reasonable suspicion that a student violated this regulation, the student Conduct Policy, or the law. The investigation will be reasonable and related to the suspected violation.

Parents have the right to request to see the contents of their student's computer files at any time.

STUDENT USE OF TECHNOLOGY (continued)

2.9 Vandalism

Vandalism, in addition to physical damage, is also defined as any malicious attempt to access, harm, alter, or destroy data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses or hacking. Any vandalism may result in the loss of computer services, disciplinary action, and/or legal referral.

2.10 Violations of this Regulation

The District will cooperate fully with local, state, or federal officials in any investigation related to any unlawful activities conducted through the District electronic infrastructure to include Internet and network access; e-mail, grading systems, data bases and user accounts.

In the event there is a substantiated claim that a student has violated the law, this regulation, or the District's student conduct policy in the student's use of the District Internet system, the student's access to the District's computer resources may be terminated and/or the student may be disciplined under applicable District policies.

2.11 Responsibility for Loss or Damages

Parents can be held financially responsible for any harm that may result from a student's intentional misuse of the system. Students may use the system only if their parents have signed a disclaimer of claims for damages against the District.

The District assumes no responsibility for the loss, destruction or theft of any personal devices including but not limited to cellular phones, computers, or personal electronic devices. School officials and District office staff are not required to investigate lost or stolen personal electronic equipment.

The District is not responsible for online material accessed off campus on a non-District network.

If a District-purchased device is checked out to a student with written parent permission for use off campus, parents can be held financially responsible for loss or damage to the device.

STUDENT USE OF TECHNOLOGY (continued)

3.0 ACTION

The principal or designee may cancel a student's user privileges whenever the student is found to have violated Board policy, administrative regulation, or the District's Student Acceptable Use Agreement. Inappropriate use may also result in disciplinary action and/or legal action, which may include suspension or expulsion, in accordance with law, school and Board policy.