STUDENT INTERNET AND SOFTWARE ACCEPTABLE USE POLICY

1.0 PURPOSE

1.1 The principal or designee establishes guidelines and limits of each school's technological resources. It is the student's personal responsibility to educate oneself on the proper and appropriate use of technology in addition to understanding the guidelines.

2.0 GUIDELINES

2.1 **The district Internet system has been established for educational purposes.** This means that students may use the system for classroom activities, professional or career development, and educational research.

2.2 *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 policy. Violations of the law or this policy may also be addressed through the district's Student Conduct and Anti- bullying Policy.

2.3 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.

3.0 Access to Online Materials

3.1 The material students may access through the district's Internet system or through the local network should be for class assignments or research related to a subject or course of study. Use for entertainment purposes, including, but not limited to personal blogging, instant messaging, on-line shopping, or gaming is not allowed, with the exception of activities created by teachers for specific instructional purposes.

3.2 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; 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.

3.3 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 policy.

4.0 Safety Requirements

4.1 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.

5.0 Unlawful, Unauthorized, and Inappropriate Uses and Activities

5.1 The following activities are unlawful, unauthorized, and/or inappropriate:

- Attempting to gain unauthorized access to the district Internet system or to any other computer system through the district Internet system is not allowed. This includes attempting to log in through another person's account or to access another person's files.
- Connecting any personal devices to the district network without express permission from the district's Technology Department is not allowed. This includes, but is not limited to cell phones, MP3 Players, and personal computers.
- 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 is prohibited.
- Using the district technology systems 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 is prohibited.
- Attempting to alter or interfere with other users' ability to post, send, receive, or submit material is not allowed.
- Attempting to delete, copy, or modify another users' work or identity is prohibited.

6.0 Inappropriate Language

6.1 Students must avoid inappropriate language in their electronic communications and 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 disruption to the school environment.
- Post photographs, video, or voice recordings of any person(s) of minor age without the consent of administration/designee.
- 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.

6.2 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.

7.0 Plagiarism and Copyright Infringement

7.1 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.

7.2 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. Questions regarding specific use of resources should be directed to the school's media resource specialist.

8.0 System Security and Resource Limits

8.1 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. Students should never demonstrate the problem to other students.

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

9.0 No Reasonable Expectation of Privacy

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

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

9.3 Parents/guardians have the right to request to see the contents of their student’s computer files at any time.

10.0 GPS Tracking Policy

10.1 Any district technology employee reserves the right to locate devices owned by the district. By agreeing to this policy, you consent to the use of your location data and services by the district for the purpose of, but not excluded to, loss and/or theft.

11.0 Vandalism

11.1 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, fines for replacement/repair, and/or legal referral.

12.0 Violations of this Policy

12.1 The district will cooperate fully with local, state, or federal officials in any investigation related to any unlawful activities conducted through the district Internet system.

12.2 In the event there is a claim that a student has violated the law, this policy, 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 the district's student conduct policy.

13.0 Responsibility for Damages

13.1 Parents can be held financially responsible for any harm that may result from a student’s intentional misuse of technology systems. Students with previous violations may regain use of the system only if their parents/guardians have signed an agreement of claims for damages against the district.

14.0 Action

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