Student Appropriate Use Policy

Violation of any part of this policy will be subject to consequences as determined by school, network, and district administration. This may include failure in citizenship, revocation of privileges, failure and/or removal from computer courses, suspension, expulsion, or other actions deemed appropriate by Cache County School District. Legal action may be taken under Utah Criminal Code Title 76 Chapter 10.

It is expected that all students sign as having read the district AUP.

Any student who utilizes the computer lab(s) or any digital equipment at the school must be aware of certain policies for use of the equipment and/or facilities. Procedures are in place for the protection of students and equipment. Students will be held accountable for any violation of the following policies (as would be the case for any classroom disciplinary matter). A student and his/her parents will be responsible for damages and will be liable for costs incurred for service or repair.

Students are only allowed to utilize the computers and network to retrieve information and run specific software applications as directed by their teacher. Students are not permitted to explore the configuration of the computer, operating system or network, run programs not on the menu, or attempt to do anything they are not specifically authorized to do.

Students are responsible for ensuring that any diskettes, CDs, memory sticks, USB flash drives, or other forms of storage media that they bring in from outside the school are virus free and do not contain any unauthorized or inappropriate files.

Safety Issues:

1. Any on-line communication should always be at the direction and with the supervision of a teacher.
2. Never provide last name, address, telephone number, or school name online.
3. Never respond to, and always report to the teacher or parent, any messages that make you feel uncomfortable or that are from an unknown origin.
4. Never send a photo of yourself or anyone else.
5. Never arrange a face-to-face meeting with someone you met on-line.
6. Never open attachments or files from unknown senders.
7. Always report to a teacher any inappropriate sites that you observe being accessed by another user or that you browse to accidentally.

Prohibited conduct includes but is not limited to the following:

1. Accessing, sending, creating or posting materials or communications that are:
    a. Damaging to another person's reputation,
    b. Abusive,
    c. Obscene,
    d. Sexually oriented,
    e. Threatening or demeaning to another person,
    f. Contrary to the school's policy on harassment, Harassing, or Bullying
    g. Illegal
2. Using the network for financial gain or advertising.
3. Posting or plagiarizing work created by another person without his/her consent.
4. Posting anonymous or forging electronic mail messages.
5. Attempting to read, alter, delete, or copy the electronic mail messages of other system users.
6. Giving out personal information such as phone numbers, addresses, driver's license or social security numbers, bankcard or checking account information.
7. Using the school's computer hardware or network for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.

8. Downloading, installing, or using games, music files, public domain, shareware or any other unauthorized program on any school's computer or computer system.
9. Purposely bringing on premises or infecting any school computer or network with a Virus, Trojan, or program designed to damage, alter, destroy or provide access to unauthorized data or information.
10. Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.
11. Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.
12. Using the school's computers or network while access privileges have been suspended.
13. Using the school's computer hardware, network, or Internet link in a manner that is inconsistent with a teacher's directions and generally accepted network etiquette.
14. Altering or attempting to alter the configuration of a computer, network electronics, the operating system, or any of the software.
15. Attempting to vandalize, disconnect or disassemble any network or computer component.
16. Utilizing the computers and network to retrieve information or run software applications not assigned by their teacher or inconsistent with school policy.
17. Providing another student with user account information or passwords.
18. Connecting to or installing any computer hardware, components, or software which is not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.
19. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.
20. Downloading or accessing via e-mail or file sharing, any software or programs not specifically authorized by Technology personnel.
21. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
22. Possessing or accessing information on school property related to "Hacking", or altering, or bypassing network security or policies.
23. Participating on message boards without teacher direction.
24. Students may use the school computer system only for legitimate educational purposes, which include class work and independent research that is similar to the subjects studied in school. Students shall not access entertainment sites, such as social networking sites or gaming sites, except for legitimate educational purposes under the supervision of a teacher or other professional.
25. All student use of the District network and Internet system or personal cell phones or other digital devices used by students while on campus is subject to the provisions of the individual school policies. Students may not share or post personal information about or images of any other student, staff member or employee without permission from that student, staff member or employee. If a student is found to have abused a personal cell phone or digital device in a manner that is not in accord with this Appropriate Use Policy, in addition to other disciplinary actions, the administrator may ban the students' use of any and all personal cell phone or digital devices.
26. Students should follow the guidelines for searching that utilize safe search engines and technology.
27. Off Campus Internet Expression -- Students may be disciplined for expression on/off campus networks or websites only if the expression is deemed to cause a substantial disruption in school, or collide or interfere with the rights of other students, staff or employees.
28. Students maintaining or posting material to a Web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students to participate fully in school or extracurricular activities is a violation of the Appropriate Use Policy and can subject the student to appropriate penalties and disciplinary action.

("Please return this section to your child's teacher or school.)

STUDENT SECTION:

Name: _____ Grade: _____ **School**: _____

(Last, First, Middle)

I have read the Cache County School District Computer and Internet Acceptable Use Policy and agree to abide by all conditions. I understand that violation of the provisions stated in the Policy may constitute suspension or revocation of computer/network/Internet privileges and/or disciplinary action.

Student's Signature: _____ **Date**: _____

SPONSORING PARENT OR LEGAL GUARDIAN SECTION:

I have read and understand the Cache County School District Computer and Internet Acceptable Use Policy. I understand that school administrators and the Cache County School District networks have taken reasonable precautions to ensure that controversial material is not accessible. Nevertheless, I understand that content which may be offensive may still be available and have discussed with my student appropriate actions to take if inappropriate content is discovered.

I give my permission for my student to use the following services at school under appropriate supervision:

❒ District computers AND Internet service.

Parent/Guardian's Signature: _____**Date**: _____

Address: _____**Phone**: _____