3095 INTERNET AND ELECTRONIC MAIL ACCEPTABLE USE POLICY

Humboldt County School District will provide employees with access to the district computer network for electronic mail and both employees and students appropriate access to the internet. Use by District employees and students must be responsible and in concert with federal and state law, HCSD Board Policies and school rules. Internet safety and responsible use will be fostered through the implementation of regulations and procedures that include technology protection measures as well as monitoring and supervision of users. Internet and public network access through the district is a privilege and requires the attached user agreement form to be signed and returned annually. (Employee Internet Acceptable Use Agreement and Student Internet Acceptable Use Agreement). This access may be revoked by the district at any time for behavior and/or actions contrary to the prescribed policy and regulation. In addition, employees in violation of this policy may be subject to disciplinary action.

Access to e-mail and the Internet will enable users to explore thousands of libraries, databases, and bulletin boards while allowing for the exchange of messages with Internet users throughout the world. While the District's intent is to make the majority of educational sites available to users, it is imperative that under the Children's Internet Protection Act (CIPA), that the district employ measures that discourage and prevent online access to harmful and inappropriate Internet sites.

Humboldt County School District will employ technology protection measures, including filtering technology, and teacher and staff monitoring use of the internet to protect children and others from depictions that are determined to be obscene, include child pornography, and may be harmful to minors. In addition, sites that promote violence, intolerance, satanic material, illegal drugs, militant extremism, and the sale, consumption or production of alcoholic and tobacco products will not be permitted.

The purpose of these technology protection measures and monitoring are to:

- Prevent minors' access to inappropriate matter on the internet and the World Wide Web.
- Prevent unauthorized access, including so-called "hacking", creation or use of proxy servers intended to bypass internet filtering and monitoring, and other activities by both employees and students that violate the law or District policies.
- Prevent the unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Prevent minors' access or exposure to materials that are harmful to themselves.

These technology protection measures apply to all computers and may be disabled, for adult use, for approved research or other lawful purposes.

Network storage areas are the sole property of the Humboldt County School District and may be subject to search. Network administrators and authorized District Personnel may review files and communications to maintain system integrity and insure that users

are using the system responsibly. As such, users should not expect that files stored on district servers are private or sole possession records.

Rules of Conduct and Compliance

Employees and students who violate the Acceptable Use Policy may have their access privileges suspended or revoked by the network administrator. In addition, further disciplinary action may be taken as permitted by district policy, school policy and applicable law.

Except as otherwise indicated below, all policies and prohibitions regarding users of the network also apply to users of individual School District computers.

1. The network may not be used to download, copy, or store any software, shareware, or freeware. In order to avoid copyright issues, this prohibition applies to any such downloading, copying or storage, regardless of copyright status, unless approved by a network administrator. Moreover, only the network administrator is authorized to consent to the terms of any software license with respect to downloaded programs.

2. With the exception of District approved educational software, users may not add any software or applications to the School District's network or computers, or add to or modify any existing software or applications, without the express permission of the network administrator. Any software which is installed must be properly licensed from the copyright owner thereof, and any modifications must comply with the terms of the applicable license(s).

3. The network may not be used for any commercial purposes.

4. The network may not be used for advertising, political campaigning, or political lobbying.

5. The network may not be used for any activity, or to transmit any material, that violates United States, Nevada State or local laws. This includes, but is not limited to; fraudulent acts, violations of copyright laws, and any threat or act of intimidation or harassment against another person.

6. The School District is a place of tolerance and good manners. Use of the network or any School District computers or facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion is expressly forbidden. Network users may not use vulgar, derogatory, or obscene language. Network users may not post anonymous messages or forge e-mail or other messages.

7. Users are strongly advised to use caution about revealing any information on the Internet which would enable others to exploit them or their identities: this includes last names, home addresses, Social Security numbers, passwords, credit card numbers or financial institution account information, and photographs. Under no circumstances should a user reveal such information about another person without that person's express or prior consent.

8. Network users may not log on to someone else's account, attempt to access another user's files, or permit anyone else to log on to their own accounts without express permission to do so in unique circumstances. Users may not try to gain unauthorized access ("hacking") to the files or computer systems of any other person or organization. However, employees must be aware that any information stored on or communicated through the School District network may be susceptible to "hacking" by a third party.

9. Network users may not access Web sites, newsgroups, or chat areas that contain material that is obscene or that promotes illegal acts. Likewise, use of the network to access or process pornographic material (whether visual or written), or material which contains dangerous recipes, formulas or instructions, is prohibited.

10. While incidental personal use of the district network by staff may be permitted, such incidental use will not be deemed a waiver of the School District's right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis. All incidental personal use is subject to the requirements of this policy. Incidental personal use is not to occur during instructional periods, or at any point in which a given staff member has oversight responsibility for students.

11. Users may not engage in "spamming" (sending irrelevant or inappropriate electronic communications individually or en masse) or participate in electronic chain letters other than for official school district purposes.

12. Users who maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data will be subject to criminal prosecution as well as to disciplinary action by the School District, up to and including termination. This includes, but is not limited to; using proxy sites to bypass filtering and/monitoring, changing or deleting another user's account; changing the password of another user; using an unauthorized account; damaging any files; altering the district network system; destroying, modifying, vandalizing, defacing or abusing hardware, software, furniture or any School District property. Users may not develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computer system (e.g., create viruses, worms) is prohibited.

13. Users may not intentionally disrupt information network traffic or crash the network and connected systems; they must not degrade or disrupt equipment or system

performance. They must not download or save excessively large files without the express approval of the network administrator.

14. Users may not plagiarize, which is a serious academic offense. Plagiarism is “taking ideas or writings from another person and offering them as your own.” Credit must always be given to the person who created the article or the idea.

15. Users may not copy any copyrighted or licensed software from the Internet or from the network without the express permission of the copyright holder: software must be approved first and then purchased or licensed before it can legally be used.

16. Users may not take data, equipment, software or supplies (paper, toner cartridges, disks, etc.) for their own personal use. Such taking will be treated as theft. Use of School District printers and paper must be reasonable.

17. Humboldt County School District assumes no responsibility for student, faculty or staff websites created and hosted outside of the district network.

Violations and Consequences

Consequences of violations include but are not limited to:

- Suspension or revocation of information network access;
- Suspension or revocation of network privileges;
- Suspension or revocation of computer access;
- Disciplinary action, up to and including termination of employment and/or services.
- Disciplinary action, up to and including suspension or expulsion.

In addition, the School District will seek monetary compensation for damages in appropriate cases. Repeated or severe violations will result in more serious penalties than one-time or minor infractions.

This Acceptable Use Policy is subject to change. The School District reserves the right to restrict or terminate information network access at any time for any reason. The School District further reserves the right to monitor network activity as it sees fit in order to maintain the integrity of the network and to monitor acceptable use. School and District-wide administrators will make final determination as to what constitutes unacceptable use.

Revised 11/26/02
Revised 2/09/10
Revised 9/13/11