

Student Use of Technology – Acceptable Use Policy

Users are expected to use technology and the Internet as an educational resource. The following procedures and guidelines are used to help ensure appropriate use of the technology and the Internet.

Jacoby Creek School District Policy:

- a. The District uses a technology protection measure that blocks or filters Internet access to some Internet sites that are not in accordance with the policy of the District and its Internet provider, the Northern Humboldt Union High School District (NHUHSD).
- b. The technology protection measure that blocks or filters Internet access may be modified by designated District staff for bona fide research purposes of an adult.
- c. Designated District staff may override the technology protection measure that blocks or filters Internet access for a student to access a site with legitimate educational value that is blocked by the technology protection measure that blocks or filters Internet access.
- d. The District and the NHUHSD staff will monitor students' use of the Internet, either through direct supervision or by monitoring Internet use history, to ensure enforcement of the policy.
- e. Not all access to the Internet or school network can be supervised.
- f. Under any circumstances, filtering technology is not perfect and therefore may in effect both interfere with educational purposes and allow some objectionable material to be viewed.

Student Technology Use Expectations:

Students are responsible for appropriate behavior on the Districts and the NHUHSD's computer network, just as they are in a classroom or on school grounds. Communications on the network/systems are often public in nature. **No assumption of confidentiality is assumed.** General school rules for behavior and communications apply. It is expected that users will comply with district standards and the specific rules set forth below. **The use of technology is a privilege, not a right, and may be revoked if abused.** The user is personally responsible for his/her actions in accessing and utilizing the school's technology resources. The students are not allowed to access, keep, or send anything that they would not want their parents or teachers to see.

The District, through its schools, shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyber bullying, and how to respond when subjected to cyber bullying.

- a. The student in whose name an online services account is issued is responsible for its proper use at all times. Students shall keep personal account numbers and passwords private and shall only use the account to which they have been assigned.
- b. Students shall use the district's system safely, responsibly, and primarily for educational purposes.

- c. Students shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs. Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)
- d. Unless otherwise instructed by school personnel, students shall not disclose, use, or disseminate personal identification information about themselves or others when using email, chat rooms, or other forms of direct electronic communication. Students also shall be cautioned not to disclose such information by other means to individuals contacted through the Internet without the permission of their parents/guardians. Personal information includes the student's name, address, telephone number, Social Security number, or other personally identifiable information.
- e. Students shall not use the system to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.
- f. Students shall not use the system to engage in commercial or other for-profit activities.
- g. Students shall not use the system to threaten, intimidate, harass, or ridicule other students or staff.
- h. Student use of district technology to access social networking sites is prohibited.
- i. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Any materials utilized for research projects should be given proper credit as with any other printed source of information.
- j. Students shall not intentionally upload, download, or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including "hacking."
- k. Students shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or use another individual's identity.
- l. Students shall report any security problem or misuse of the services to the teacher or principal.
- m. Students may bring personal technology, including computers, smart phones, network access devices, or other electronic signaling devices to school provided that such technology is used for instructional purposes. Students shall abide by the instructions provided by teachers and other school staff in the use of such personal technologies. Access to the Internet or other District communication systems for personal technology is limited to wireless access points, where available, on the school campuses or other access devices away from school. Access to the Internet or other District communication systems from personal technology **is not available via hardwire connections** and no physical connection points on the campus are allowed by any non-school owned equipment. Student-owned devices must have up-to-date anti-malware/anti-virus software installed as appropriate and available for each device. In addition, the District will not be liable or responsible for any losses or damages resulting from any such malware/virus that may be propagated to the student-owned device while connected to the District network.
- n. The use of District technology resources may involve the use of a password, network access code or other identifying or validating code. Such passwords and codes are to be protected as private information provided to the individual user for their sole purpose. Such passwords and codes **shall not** be disclosed by the student to others.
- o. As stated above, the use of JCSD technology resources is not private; students should not expect that files stored on or transmitted via the District's resources will be confidential. All digital transmissions are subject to inspection and/or monitoring by District employees and

other officials. Digital storage is JCSD owned or licensed to maintain system integrity and ensure that students are using technology responsibly.

Not all access to the Internet can be supervised. Students agree not to send, access, submit, publish, display or print over the Internet or JCSD network, or using JCSD technology resources, any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive or illegal material. Cyber bullying is specifically prohibited. It shall be the student's responsibility to report the inappropriate use, web site, or communication to the student's teacher or other staff member.

The district reserves the right to monitor use of the district's systems for improper use without advance notice or consent. Students shall be informed that computer files and electronic communications, including email, are not private and may be accessed by the district for the purpose of ensuring proper use.

Whenever a student is found to have violated Board policy, administrative regulation, or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

Limitations of Liability:

The district shall not be responsible for any damages suffered by the student, including those arising from non-deliveries, miss-deliveries, service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the student's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. The District assumes no liability for personal technology, including computers, smart phones, network access devices, or other electronic signaling devices, if such devices are damaged, lost, or stolen. The student and his/her parent/guardian shall indemnify and hold the District harmless from any losses sustained as the result of use or misuse of district's technology resources by the student, and/or the loss or damage of personal technology.

Consequences of Misuse and/or Violation of the Provisions of this Agreement:

Misuse of personal or JCSD and personal technology resources on or near school property, in school vehicles, at school-sponsored activities, as well as using district technology resources via off-campus remote access, may result in disciplinary action up to and including expulsion from the schools of the district. This Agreement shall be used in conjunction with JCSD Board of Education policies, California Education Code, and other local, state and federal laws and regulations governing the applicable manner.

Students, parents, and guardians should recognize that the nature of the use of District technology resources extends outside of the school itself and into off campus remote locations such as homes. The JCSD's jurisdiction to enforce student behavior and discipline policies and rules shall apply whether the misuse is at school or away from school as long the JCSD's technology resources are being used in the inappropriate behavior.

1st Reading:

2nd Reading:

Adopted: