



## **Nevada Joint Union High School District**

### **9-12 Student Instructional Technology Acceptable Use and Internet Safety Policy**

Technology provides a wealth of educational opportunities for staff and students. Access to these vast resources requires responsible use by each individual. It is important that you understand your rights and privileges when using the Nevada Joint Union High School District (NJUHSD) resources in this environment. This document describes the computer, network, and Internet resources made available by the school and your responsibilities and obligations in the use of these resources.

#### **Introduction**

NJUHSD is pleased to offer students access to district devices, communications systems<sup>1</sup>, the Internet, and an array of technology resources to promote educational excellence. Each student must act in an appropriate manner while using district or personal technology resources consistent with school, district, and legal guidelines whether on or off campus. It is the joint responsibility of school personnel and the parent or guardian of each student to educate the student about appropriate digital citizenship and to establish expectations when using technology.

District technology resources are provided to students to conduct research, complete assignments, and communicate with others in furthering their education. Students may not offer or provide products or services through the NJUHSD network system. The NJUHSD network system has not been established as a public access service or a public forum. Access is a privilege, not a right; as such, general rules of school behavior apply. Access to these services is given to students who agree to act in a considerate and responsible manner. Students must comply with school standards and honor this agreement to be permitted the use of technology. Disciplinary action may be taken against students for misuse of computer, network, and information resources. Students using a personal device on campus will be deemed an “authorized user” and will grant access to the personal device to district staff upon reasonable suspicion of wrongdoing.

<sup>1</sup>(Communication systems include Learning Management system (LMS), e-mail, web sites, blogging, podcasting, forums, wikis, and/or other emerging technologies).

#### **Use of NJUHSD Network**

- Each student, along with a respective parent/guardian, must sign an Acceptable Use Policy (AUP) Agreement to be granted an account on the NJUHSD network system.
- Students will not make deliberate attempts to disrupt or harm the computer system and its hardware or destroy data by spreading computer viruses or by any other means. Use or possession of “hacking” tools are prohibited.

- Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a student provide their password to another person except to a school administrator or parent.
- Students will not attempt to log on or connect to the NJUHSD network under any identity other than their own username.
- Students will not attempt to gain unauthorized access (including hacking) to the NJUHSD network system or to any other computer system through the NJUHSD network system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are inappropriate, even if only for the purposes of "browsing" and may result in disciplinary action.
- Students will immediately notify a teacher if they have identified a possible security problem.
- Students will use school resources (e.g. printers, cameras, etc.) only for educational purposes.
- Students will not download or upload unauthorized programs or files that can be run or launched.
- Use of NJUHSD computers, network, and Internet services does not create any expectation of privacy.
- Students should expect routine monitoring of computer usage and Internet browsing while logged on to the NJUHSD network.
- Parents have the right to request to see the contents of student files.

## **Internet Access**

- All students will have access to Internet resources through devices connected to the network.
- NJUHSD actively uses filtering software to meet the Children's Internet Protection Act (CIPA) requirement and to prevent students from accessing graphics that are (1) obscene, (2) pornographic, or (3) harmful to minors. NJUHSD retains the right to block unacceptable web sites. Filtering software is not a perfect science and it may be possible for users to access inappropriate sites.
- NJUHSD does not guarantee network functionality or accuracy of information.
- Students will not use the NJUHSD network system to access inappropriate material including sites that display profane or obscene (pornography) material, advocates illegal acts, encourages the use of drugs, alcohol or tobacco, school cheating, weapons, material that advocates violence, participation in hate groups or discrimination towards other people, or other inappropriate activities considered harmful to minors.
- If students mistakenly access inappropriate information, they should immediately minimize their screen and tell their teacher. This will protect the student against a claim that they have intentionally violated this Policy.
- The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

## **Use of Messaging Services<sup>2</sup>**

- An E-mail account will be provided to students for educational purposes and not as a public or student forum.
- Students will promptly disclose to their teacher or other school employee any message or information they receive that is inappropriate or makes them feel uncomfortable while on the web, using e-mail, chat rooms, forums or other forms of messaging services.
- E-mail may not be used for unlawful activities, political or commercial purposes, any form of harassment or threats, sending of spam messages or chain letters to more than five people or any use that interferes with the school computing services or its employees.
- Students may not send messages with a false identity or alter forwarded mail out of context.
- Students will abide by rules of network etiquette by not using defamatory, inaccurate, abusive, obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or prejudicial language in public or private communication.
- Students will not post personal contact information about themselves or other people without parental approval. Personal contact information includes, but is not limited to, names, home, school, parent work addresses, telephone numbers, personal photos or videos.

- Students will not repost a message that was sent to them privately without permission of the person who sent them the message.
- Students will not post or share information that could cause damage or a danger of disruption to NJUHSD schools or any other organization or person.

<sup>2</sup> (LMS, e-mail, chat, forums, blogs, social networking, instant message, SMS, and other forms of messaging services)

## **Educational Applications<sup>3</sup>**

Students will follow all established Internet safety guidelines including the following conditions:

- The use of digital media is considered an extension of your classroom. Any speech that is considered inappropriate in the classroom is also inappropriate in all digital environments. This includes, but is not limited to, profanity, racist, sexist or discriminatory remarks.
- Students using digital media are expected to act safely by keeping ALL personal information out of their posts.
- A student should not post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
- Never link to web sites from your digital environment without reading the entire article to ensure it is appropriate for a school setting.
- Students using such tools agree to not share their username or password with anyone besides their teachers and parents and treat digital spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate online.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse according to the school discipline policy.

<sup>3</sup> (LMS, e-mail, chat, forums, blogs, social networking, instant message, wikis, and other forms of collaborative software)

## **Teacher Responsibilities**

- Teachers will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the district curriculum.
- Classroom use of networked resources will be in support of educational goals.
- Teachers will provide alternate activities for students who do not have permission to use the Internet.
- Teachers will make every effort to protect student data privacy when using educational applications.

## **Cyberbullying**

NJUHSD expressly forbids cyberbullying. For the purposes of this policy, “cyberbullying” shall mean using messaging services<sup>2</sup> and/or other digital communication devices to bully others by:

- Sending or posting cruel messages or images;
- Threatening others;
- Excluding or attempting to exclude others from activities or organizations;
- Starting or passing on rumors about others or the school system;
- Harassing or intimidating others;
- Sending angry, rude or vulgar messages directed at a person or persons privately or to an online group;
- Sending or posting harmful, untrue or cruel statements about a person to others;
- Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger;
- Sending or posting material about a person that contains sensitive, private or embarrassing information, including forwarding private messages or images;
- Engaging in tricks to solicit embarrassing information that is then made public;

- Using camera and/or video enabled devices to bully another person or to invade another person's privacy.

## **Privacy, Plagiarism, Piracy and Copyright Infringement**

- An image taken by any camera or video enabled device may not be published, broadcast, or transmitted to any other person, by any means, without the knowledge and consent of each person appearing in that image who had a reasonable expectation of privacy at the time the image was recorded or the person who owns the copyright in the material appearing in that image.
- Camera and/or video enabled devices may not be used in any classroom without a teacher's permission.
- Students will not plagiarize works that they find on the Internet.
- Students will not download or install pirated software, music, video or files that infringe on copyright laws onto computers. Possession of unlicensed or pirated software is illegal.
- Students will respect the rights of copyright owners.

## **Use of School Hardware<sup>4</sup>**

- School mobile devices will not be left unattended. Students are responsible for the care of their assigned mobile device.
- In the event of any damage to a school device, the student agrees to inform their teacher or Technology Site Contact so that repairs can be performed.
- The student and parent/guardian will be held financially liable for damage or loss of the chromebook package.
- If the District reasonably determines that the student has willfully damaged any school hardware, the District reserves the right to apply the liability provisions of Education code section 48904.

<sup>4</sup>(Hardware systems include laptops, digital camera/video equipment and/or other technologies).

## **Consequences**

- In the event there is a claim that a student has violated this policy in the use of the NJUHSD network system, the student will be provided with a written notice of the suspected violation and an opportunity to present an explanation before an administrator.
- If a student is found to have violated this Policy, the consequences will be, but not limited to, warnings, usage restrictions being placed on their network account, or disciplinary action at the discretion of the site administration.
- A violation of Federal, State or local laws or ordinances may result in legal proceedings.