

HAPPY VALLEY ELEMENTARY SCHOOL DISTRICT

Acceptable Use Standards

These AUS (Acceptable Use Standards) serve as notice to users, in compliance with Education Code Sections 48980 and 51871.5, of the Happy Valley Elementary School District policies regarding information technology use, computer use, and access to the Internet for its students, employees and other authorized users.

ACCEPTABLE USE STANDARDS FOR COMPUTER USE

In support of the Happy Valley Elementary School District's mission of promoting quality service and lifelong learning, HVESD provides computing, networking, and information resources to the campus community of students, faculty, and staff.

This AUS applies to use of all HVESD computing and information technology resources of any kind. Additional computer and network use policies, terms and conditions may be in place for specific electronic services offered by HVESD.

Rights and Responsibilities

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, the integrity of the systems, related physical resources, and observe all relevant laws, regulations, and contractual obligations.

It is the understanding that HVESD provides its employees with computers and network connectivity for the express purpose of fulfilling their professional and academic responsibilities. Any use of information technology resources deemed unacceptable is subject to disciplinary action.

Students and employees may have rights of access to information about themselves contained in electronic media, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files, as required, to protect the integrity of information technology resources. For example, following organizational guidelines, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that may have been corrupted or damaged.

Existing Legal Context

All Federal and State laws, as well as, Happy Valley Elementary School District's rules, regulations and policies apply. Applicable laws and regulations are not limited to those specific to information technology resources, but also include those that may apply generally to personal and professional conduct.

Misuse of computing, networking, or information resources may result in the restriction of privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable Happy Valley Elementary School District or school policies, procedures, or collective bargaining agreements.

Complaints alleging misuse of campus information technology resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. copyright law and is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of Misuse

Examples of misuse include, but are not limited to, the following activities:

- Using an information technology account that you are not authorized to use.
- Obtaining a password for an information technology account without the consent of the account owner.
- Allowing anyone other than you, including other staff members and students use of your HVESD password including access to any educational programs.
- Using the HVESD network to gain unauthorized access to any computer system(s) or to view files or information that you are not authorized to use.
- Removal, alternation, or destruction of sensitive or confidential information including but not limited to personnel or student records.
- Knowingly performing an act which will interfere with the normal operation of information technology resources, including but not limited to computers, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user; a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to programs known as computer viruses, Trojan horses, malware, worms, or anything that might cause a denial or interruption of service.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting information technology resources.
- Using electronic mail or other communications to harass others.
- Masking the identity of an account or machine.
- Posting materials to bulletin boards, social media sites, or to other information technology that violate existing laws or HVESD codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files, or software without the explicit agreement of the owner.
- Use of information technology resources for commercial gain to the user or for purposes unrelated to the user's employment, education, or needs.
- Excessive personal use or personal use during work hours or instructional time, or personal use that interferes with the orderly conduct of the HVESD in any way.

Activities will not be considered misuse when authorized by appropriate HVESD officials, or their designees, for investigations, security or performance testing.

ACCEPTABLE USE STANDARDS FOR INTERNET USAGE

The Internet may contain harmful matter as defined in section 313(a) of the Penal Code, or may contain material considered by persons viewing it as harmful. Although we exercise reasonable supervision over those who access the Internet within our system including exercising due diligence in educating students and employees regarding acceptable and unacceptable practices on the Internet within our system, it is still possible that authorized users may intentionally or unintentionally access information which some may consider to be inappropriate.

Acceptable Use Standards

- The Happy Valley Elementary School District may terminate a user's account at any time if these Acceptable Use Standards are violated.

- Use of the system is a privilege, which may be terminated if the user abuses the system. Abuse would include, but is not limited to: the placing of unlawful information on or through the system; the use or retrieval of information (messages, text, images, and programs) which is obscene, abusive, or otherwise objectionable; redistribution or extension of Internet connectivity beyond the user's computer; and use of the system as a commercial operation.
- The Happy Valley Elementary School District or designated staff, will determine what constitutes use or retrieval of information (messages, text, images, programs), which is obscene, abusive, or otherwise objectionable.
- The Happy Valley Elementary School District or designated staff reserves the right to access any material stored in its equipment and reserves the right to remove any material which it considers obscene, abusive, or otherwise objectionable. Access may occur at any time without advance notice to the user.
- Each user is responsible for any password security extended to him or her in conjunction with Internet access or activities.

USE OF PERSONAL SOCIAL NETWORKING SITES

As an organization with a mission to support the education of young people and as a longtime leader in educational technology, HVESD's standards for appropriate online communication are necessarily high. One of the challenges of the digital age is that everything we write or post online leaves a long-lasting and even permanent record that potentially can be seen by students, their families, and other members of HVESD's extended community. This is particularly true with social networking and media sites.

While the organization respects the right of employees to use social media and networking sites, as well as personal websites and blogs, it is important that employee's personal use of these sites does not damage the HVESD's reputation, its employees, or its students or their families. Employees should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding that what is private in the digital world often has the possibility of becoming public, even without their knowledge or consent. All online behavior should be consistent with standards of professionalism expected of HVESD employees.

Happy Valley Elementary School District strongly encourages all employees to carefully review the privacy settings on any social media and networking sites they use (such as Facebook, MySpace, Twitter, Flickr, LinkedIn, etc.), and exercise care and good judgment when posting content and information on such sites. When using a social media site, an employee is encouraged to carefully consider the consequences if the employee includes current students, co-workers, or other work-related acquaintances as "friends," "followers" or any other similar terminology used by various sites. If an employee has a community that extends to persons who are parents or other members of HVESD's community, s/he must exercise good judgment and use professional, age-appropriate behavior regarding any content that is shared on the site. Additionally, employees should adhere to the following guidelines, which are consistent with the HVESD's workplace standards on harassment, student relationships, conduct, professional communication, and confidentiality:

- ♦ An employee may not "Friend" or include students in personal social networks ie., Facebook, My Space, Google Circles, Pinterest, SnapChat, Instagram, etc.

- ♦ An employee should not make statements that would violate any HVESD's policies, including its policies concerning discrimination or harassment;
- ♦ The employee must uphold HVESD's value of respect for the individual and avoid making defamatory statements about past or present employees or students, or their families;
- ♦ An employee may not disclose any confidential information of the HVESD or confidential information obtained during the course of his/her employment, about any individuals or organizations, including students and/or their families.

If HVESD believes that an employee's activity on a social networking site, blog, or personal website may violate the HVESD policies, HVESD may request that the employee cease such activity. Depending on the severity of the incident, the employee may be subject to disciplinary action.