EUREKA COUNTY SCHOOL DISTRICT

INFORMATION TECHNOLOGY

The District requires employees to use information technology (computer systems, telecommunication, and other devices, and electronic information/communication) responsibly, and in a manner which is not detrimental to the mission and purpose of District.

Employees are prohibited from using information technology in any way which violates District policy or procedure. Employee use of the District's information technology to engage in such conduct, or engaging in such conduct using personal information technology devices while on duty can create liability for District, and as such, obligates District to undertake reasonable procedures to investigate such allegations, including but not limited to inspection of information technology equipment. In the event an employee becomes the subject of such an investigation and the allegations include potential violations of District policies, the District will undertake such an investigation and inquiry by all means allowable under state and federal law.

Privacy

Employees should not expect privacy with respect to any of their activities when using the District's computer and/or telecommunication property, systems, or services, even when accessing them from a personal device. Use of passwords or account numbers by employees does not create a reasonable expectation of privacy and confidentiality of information being maintained or transmitted. The District reserves the right to review, retrieve, read, and disclose any files, messages, or communications that are created, sent, received, or stored in the District's network, or on the District's computer systems and/or equipment. The District's right to review, also called monitoring, is for the purpose of ensuring the security and protection of business records, preventing unlawful and/or inappropriate conduct, and creating and maintaining a productive work environment.

In accordance with provisions of NRS 613.135, District will not request user names and passwords for employees' personal social media accounts and will not take any type of employment action against an employee who refuses to provide the user name and password for their personal social media account. This provision does not prevent the District from requiring an employee to disclose the user name and password for access to the District's computer or information system.

ADOPTED: 10/8/96
REVISED: 12/6/96
REVISED: 8/14/01
REVISED: 8/13/19

Acceptable Use

a. District computers, associated hardware, software, and services, including, but not limited to, electronic mail and access to online services, as well as voice mail and faxes, even when accessed from a personal device, belong to the District and, as such, are provided for business use. Very limited or incidental use of District-owned equipment by employees for personal, non-business purposes is acceptable as long as it is

   1) Conducted on personal time (i.e., during designated breaks or meal periods);
   1) Does not consume system resources or storage capacity;
   2) Does not involve any prohibited uses; or
   3) Does not reference the District or themselves as an employee without prior approval. This includes, but is not limited to:
      i. Text which identifies the District;
      ii. Photos which display District logos, patches, badges, or other identifying symbols of the District;
      iii. Information of events which occurs involving the District without prior approval, or
      iv. Any other material, text, audio, video, photograph, or image which would identify the District.

b. Downloading and/or installing software, applications, or programs on District devices is prohibited unless pre-approved by the District Systems Engineer.

c. Employees may use information technology, including the Internet, World Wide Web, social media sites during work hours on job-related matters to gather and disseminate information, maintain their currency in a field of knowledge, participate in professional associations, and communicate with colleagues in other organizations regarding business issues.

d. An employee's use of the District's computer systems, telecommunication equipment and systems, and other devices or the employee's use of personally-owned electronic devices to gain access to District's files or other work-related materials maintained by District constitutes the employee's acceptance of this policy and its requirements.

e. All wired and wireless connectivity using district network structures, whether on district-provided or personal devices is subject to the provisions of this policy.

ADOPTED: 10/8/96
REVISED: 12/6/96
REVISED: 8/14/01
REVISED: 8/13/19

Prohibited Use

Prohibited use includes, but is not limited to, the following:

a. Sending, receiving, or storing messages or images that a "reasonable person" would consider to be offensive, disruptive, harassing, threatening, derogatory, defamatory, pornographic, indicative of illegal activity, or any that contain belittling comments, slurs, or images based on race, color, religion, age, gender, pregnancy, sexual orientation, national origin, ancestry, disability, veteran status, domestic partnership, genetic information, gender identity or expression, political affiliation, or membership in the Nevada National Guard.

b. Subscriptions to newsletters, advertising, "clubs," or other periodic e-mail which is not necessary for the performance of the employee's assigned duties.

c. Engaging in political activities including, but not limited to, solicitation or fund raising.

d. Engaging in religious activities including, but not limited to, proselytizing or soliciting contributions.

e. Conducting outside employment in any manner.

f. Engaging in illegal, fraudulent, defamatory, or malicious conduct.

g. Writing or participating in social media in a way that injures, disparages, and/or defames the District or any of its schools, members of the public, and/or its employees' reputations by name or implication.

h. Downloading, uploading, or otherwise transmitting without authorization:

    - Confidential, proprietary information, or material
    - Copyrighted material
    - Illegal information or material
    - Sexually explicit material

i. Obtaining unauthorized access to other systems.

j. Using another person's password or account number without explicit authorization by the District.

ADOPTED: 10/8/96
REVISED: 12/6/96
REVISED: 8/14/01
REVISED: 8/13/19

k. Improperly accessing, reading, copying, misappropriating, altering, misusing, or intentionally destroying the information/files of the District and other users.

l. Loading unauthorized software or software not purchased or licensed by the District.

m. Breaching or attempting to breach any security systems or otherwise maliciously tampering with any of the District's electronic systems including, but not limited to, introducing viruses.

n. Using the District's information technology for personal, non-business purposes in other than a very limited or incidental way.

o. Using a District email address to register on personal/private websites.

ADOPTED: 10/8/96
REVISED: 12/6/96
REVISED: 8/14/01
REVISED: 8/13/19