Employee Information Technology Acceptable Use Policy (AUP)

The Elko County School District provides computers, networks, Internet, media retrieval, satellite and other telecommunication access (Information Technology) to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff.

Employees are to utilize the District's Information Technology services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

All District information technology equipment remains under the control, custody and supervision of the District. The District reserves the right to monitor activity by all employees. Employees have no expectation of privacy in their use of school computers.

The Superintendent shall be responsible for overseeing the implementation of this policy, and for advising the Board of the need for any future amendments or revisions to the policy. The Superintendent may develop additional administrative procedures governing the day-to-day management and operations of the District's Information Technology system as long as they are consistent with the Board's policy. The Superintendent may delegate specific responsibilities to administrative staff and others as the Superintendent deems appropriate.

The intent of these Board-level policies is to provide employees with general requirements for utilizing the District's Information Technology services. The Board policies may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the computer system. These policies provide general guidelines and examples of prohibited uses for illustrative purposes, but do not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the system administrator or site administrator. Failure to comply with this Board policy or other established procedures or rules governing information technology use may result in disciplinary action, up to and including discharge. Illegal uses of the District's Information Technology will also result in referral to law enforcement authorities.

Use Policies:

A. Access to School Computers, Networks, Internet Services, Media Retrieval, Satellite and Telecommunications

1. The school district, through the Nevada School Network, the Department of Education, and in cooperation with UNR/Great Basin College is providing access to the Internet, email and interactive compressed video for Elko

County School District employees.
2. The level of access that employees have is based upon specific employee job requirements and needs.

B. Acceptable Use

Employee access to the District's Information Technology services is provided for administrative, educational, communication and research purposes consistent with the District's educational mission, curriculum and instructional goals. General rules and expectations for professional behavior and communication apply to its use.

C. Prohibited Use

The employee is responsible for his/her actions and activities involving telecommunication, satellite, media retrieval, computers, networks and Internet services, and for his/her computer files, passwords and accounts. General examples of unacceptable uses which are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or in violation of other Board policies, including sending, receiving, or storing messages that a “responsible 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, sex, sexual orientation, age disability, or national origin;

2. Sending or storing messages or images that would offend or harass on the basis of race, sex, sexual orientation, religion, age, political belief, or disability;

3. Any receipt of inappropriate email must be reported to immediate supervisor in printed form. Recipients of inappropriate email must not delete these types of email from their computer. This will allow District computer technicians access to the email electronically, and will help them to successfully track the sender.

4. Any inappropriate communications with students or minors;

5. Any use for private financial gain, or commercial, advertising or solicitation purposes;

6. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students and/or their families for

non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.

7. Any communication that represents personal views as those of the District or that could be misinterpreted as such;

8. Downloading or loading software or applications without permission from the Director of Technology, site administrator or designee;

9. Intentionally forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;

10. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the Director of Technology, site administrator or designee. Policies that regulate normal mail use are in effect when using mass emails.

11. Any malicious use or disruption of the District's computers, networks and Internet services or breach of security features;

12. Any misuse or intentional damage to the District's computer equipment;

13. Misuse of the computer passwords or accounts (employee or other users);

14. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;

15. Any deliberate attempt to access unauthorized sites;

16. Failing to report a known breach of computer security to the Director of Technology, site administrator, or designee;

17. Using school computers, networks and Internet services after such access has been denied or revoked; and

18. Any attempt to delete, erase or otherwise conceal any information stored on a school computer that violates this policy. The use of hard drive scrubbers is prohibited. A person who immediately deletes inappropriate material is not in violation of this policy.

D. No Expectation of 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. 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 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.

E. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

F. Staff Responsibilities to Students

Teachers, staff members and volunteers who utilize information technology for instructional purposes with students have a responsibility to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the District's policies and rules concerning information technology use and to enforce them. When, in the course of their duties, employees/volunteers become aware of student violations, they are expected to stop the activity and inform the site administrator.

G. Compensation for Losses, Costs and/or Damages

The employee shall be responsible for any losses, costs or damages incurred by the District related to violations of this policy.

H. District Assumes No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The District assumes no responsibility for any unauthorized charges made by employees, including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

I. Violation of Policy

Improper or prohibited use of the District's property, systems, or services will result in discipline, up to and including termination.