**LYON COUNTY SCHOOL DISTRICT**
**BOARD POLICY _____GBBP**

## INFORMATION TECHNOLOGY

The District requires employees to use information technology (computer systems, telecommunication, other devices, and electronic information/communication) responsibly, and in a manner which is not detrimental to the mission and purpose of the District. To maintain a level of professionalism, any publication through any means (electronic or otherwise), which is potentially adverse to the operation, morale, or efficiency of the District, will be deemed a violation of this policy.

Employees are prohibited from engaging in any conduct ~~which would~~ that violates District policy or procedure. Use of personal or District electronic devices to engage in such conduct can create liability for the District, and as such, obligates the District to undertake reasonable procedures to investigate allegations, including but not limited to the inspection of the equipment. In the event an employee becomes the subject of such an investigation and the allegations include potential violations of District policies, whether on work or personal time, and whether using District or personal devices, the District will undertake an investigation and inquiry by all means allowable under state and federal law.

The District will periodically provide cybersecurity training to ~~all employees on this policy and best practices in preventing~~ educate employees about the dangers of phishing ~~attempts~~, ransomware infections, ~~or~~ and social engineering ~~attempts~~.

**Reference:** NRS 613.135 and 391

***INFORMATION TECHNOLOGY - ADMINISTRATIVE REGULATIONS***

1. Privacy

Employees ~~should~~ have not expectation of privacy ~~with respect to any of~~ regarding their activities when using the District's ~~computer and/or telecommunication property,~~ systems~~, or services,~~ even when ~~accessing from a~~ using personal devices. 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~~ monitor~~ing, 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~~ communications and file activity in compliance with privacy laws.

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

2. Use

The computers, associated hardware and software including, but not limited to, electronic mail (e-mail or instant messaging "IM") and access to online services, as well as voice mail, pagers, smart phones 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:

a) Is conducted on personal time (i.e., during designated breaks or meal periods);
b) Does not consume system resources or storage capacity;
c) Does not involve any prohibited uses; and
d) Does not reference the District or themselves as an employee without prior approval, including, but not limited to:

- Text which identifies the District;

- Photos which display District logos, patches, badges, or other identifying symbols of the District;
- Information of events which occurs involving the District without prior approval
- Any other material, text, audio, video, photograph, or image which identify the District.

Employees loading, importing, or downloading files from sources outside the District's system, including files from the Internet, World Wide Web, social media sites, and any computer disk, must ensure the files and disks are scanned with the District's current virus detection software before installation and execution. Compliance to copyright or trademark laws prior to downloading files or software must be adhered to explicitly.

Employees may use information technology, including the Internet, World Wide Web, and 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.

An employee's use of the District's computer systems, telecommunication equipment and systems, other District 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 the District constitutes the employee's acceptance of this policy and its requirements.

Employees must ~~receive permission and~~ attain authorization from their administrator or manager/supervisor ~~or~~ and the District Information Technology (IT) Manager prior to~~:~~

- ~~I~~installing copyrighted software to ensure the District has an active license~~;~~ and
- ~~D~~distributing or copying property protected by copyright, trade secret, patent, or other intellectual property.

Personal use must not occur during working hours (except for lunch/break periods), reference the District without approval, and/or consume excessive District resources.

3. Prohibited Activities

The following activities are strictly forbidden by this policy:

a. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations,

including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the District.

b. Unauthorized copying of copyrighted material including but not limited to digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the District or the end user does not have an active license.

c. The installation of software on District computers without the prior approval of the IT Manager is prohibited.

d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The District IT Manager should be consulted prior to export of any material that is in question.

e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs).

f. Allowing access to confidential or proprietary information on District systems. This includes family and other household members when work is being conducted at an employee's home.

g. Using District equipment or systems to actively engage in procuring or transmitting materials that are in violation of harassment or employee bullying policies and the laws of the State of Nevada.

h. Making fraudulent offers of projects, items or services originating from any District account.

i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

j. Effecting security breaches or disruptions of network communication.

k. Port scanning or security scanning, unless conducted by or on behalf of the IT Manager or designee during duties performed on behalf of the District.

l. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.

m. Circumventing user authentication or security of any host network or account.

n. Interfering with or denying service to any user other than the employee's host (e.g., denial of service attack).

o. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/intranet/extranet.

p. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e.g., email spam).

q. Any form of harassment or bullying via email, telephone or text, whether through language, frequency or size of messages.

r. Unauthorized use, or forging, of email header information.

s. Solicitation of email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

t. Creating or forwarding "chain letters" or "Ponzi" or other pyramid schemes of any type.

u. Use of unsolicited email originating from within the District's networks or other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by the District or connected via the District's network.

v. Physical alteration or repair of any hardware or software such as computers, laptops, printers, fax machines, phones, online services, email systems, bulletin board systems, recording equipment, copiers, or any other software that is owned, licensed by or operated by the District, as well as monitors, mice, keyboards; users must report any problems with hardware or software to the District help desk ticket system.

4. Permitted Activities

Use of District computers and electronic communications resources are for program and business activities of the District. All use of such resources shall be conducted in a framework of honest, ethical and legal activities that conform to applicable license agreements, contracts, and policies regarding their intended use. ~~Although incidental and occasional personal use of the organization's communications systems are permitted, users automatically waive any rights to privacy.~~ Employees consent to District monitoring by using District systems, even for limited personal use.

5. Artificial Intelligence Acceptable Use

a. Regulation

This regulation outlines ~~the guidelines and regulations for the appropriate use of Artificial Intelligence (AI) for the District. Its purpose is to ensure~~ the responsible, ~~and~~ ethical, and legal use of artificial intelligence (AI) technologies ~~to protect the rights and privacy interests of District staff, and the public it services~~.

b. Purpose

The purpose of this regulation is to establish the rules for acceptable use of the recent growth of AI technologies relating to District information resources. This regulation applies to all employees, contractors, and third-party vendors who utilize AI technologies on behalf of the District. It encompasses all AI systems, applications, and application programming interfaces (APIs), including, but not limited to, ChatGPT, Gemini, ~~and~~ image generators, and other machine learning algorithms, natural language processing, computer vision, and robotic process automation, ensuring AI technologies are used in a manner that aligns with the District's core values and mission, promoting transparency, accountability, and public trust in our AI initiatives.

c. Responsible Use of AI

- *General Rule:* Employees may use AI technologies to create work-related content or complete work tasks under the supervision of their administrator/supervisor and District administration.
- *Lawful Use:* AI technologies are quickly evolving and should be used in compliance with all applicable laws, regulations, and policies. Any use that violates legal requirements or infringes upon the rights of individuals is strictly prohibited. NRS 391 prohibits AI from performing the functions and duties of a school counselor, school psychologist, or a school social worker.
- *Data Privacy and Security:* All AI activities must prioritize the protection of personal information and respect privacy rights. Any data collected or processed by AI systems should be handled in accordance with relevant privacy and security policies. Uploading personally identifiable or confidential information into AI systems is strictly prohibited.
- *Transparency and Explainability:* Whenever AI systems are deployed, efforts should be made to cite them appropriately, ensuring transparency and explainability. Users should have access to information regarding the functioning of AI systems, the data used, and the algorithms applied.
- *Bias Mitigation/Fairness and Equity:* AI systems should be designed and implemented with measures to mitigate bias. Special attention should be given to promote fairness and equity, and avoid discrimination based on race, gender,

religion, or any other protected characteristics. Bias mitigation efforts should be included in the prompt and may be subject to review.

- *Human Oversight:* AI should be used as a tool to assist decision-making, and human oversight should be maintained. Final decisions should not solely rely on AI outputs and should involve critical evaluation by qualified individuals.
- *Accountability:* Individuals responsible for the use, development, deployment, and maintenance of AI systems will be accountable for their actions. They should ensure that AI systems are designed to minimize harm and maximize benefits for all stakeholders.

d. Responsible Data Usage

- *Data Collection and Consent:* Data collection through AI systems must be limited to what is necessary for the intended purposes. Appropriate consent should be obtained from individuals when their personal data is being processed.
- *Data Quality and Integrity:* AI systems should be developed using accurate and reliable data. Efforts must be made to ensure data integrity, prevent data tampering, and maintain data quality throughout the AI lifecycle. AI platforms may produce inaccurate results, warranting cross-reference and validation.
- *Data Retention and Disposal:* Personal data collected by AI systems should be retained only for as long as necessary and securely disposed of when no longer needed according to District policy.
- *Personal Identifying Information:* The uploading of any personal identifying information is strictly prohibited when using any AI system.

e. Reporting Violations

Employees must immediately report any actual or perceived violations of this policy to their immediate administrator, supervisor, manager, or the Executive Director of Human Resources.

f. Training

AI is growing rapidly and being integrated into existing architecture during vendor updates to hardware, software, and firmware. Regular monitoring~~,~~ ~~training,~~ and ~~awareness programs on~~ AI ethics training ~~and responsible use~~ will be provided to employees.

g. Violations of Policy

Employees in violation of the provisions of this policy may be subject to disciplinary action, up to and including termination.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

~~By adhering to this policy, the District demonstrates its commitment to responsible AI use, ethical conduct, and the protection of individual rights and privacy.~~