LYON COUNTY SCHOOL DISTRICT
BOARD POLICY _____GBBP

INFORMATION TECHNOLOGY

The District requires employees to use information technology (computer systems, telecommunication and other devices, and electronic information) responsibly, and in a manner, which is not detrimental to the mission and purpose of 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 District, will be deemed a violation of this policy.

Employees are prohibited from engaging in any conduct which would violate District policy or procedure. Use of personal or District cell phones or other 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 such allegations. Cell phones or other electronic devices that are owned by the district or for which the employee is reimbursed are subject to inspection. Personal cell phones or other electronic devices can only be accessed with the express written consent of the employee. 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 such an investigation and inquiry by all means allowable under state and federal law.

Policy #GBBP
Revised 11/24/15

INFORMATION TECHNOLOGY – ADMINISTRATIVE REGULATIONS

1. 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, including the use of personal e-mail accounts on the District's electronic 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 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 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.

2. Use

   - The computers, associated hardware and software, including electronic mail (e-mail or instant messaging) and access to online services (the Internet), as well as voice mail, pagers, smart phones and fax machines, belong to the District and, as such, are provided for business use. Very limited or incidental use by employees for personal, non-business purposes is acceptable as long as it is

     a) Conducted on personal time (i.e., during designated breaks or meal periods),

     b) Does not consume system resources or storage capacity, and

     c) Does not involve any prohibited uses.

   - Employees loading, importing, or downloading files from sources outside the District's system, including files from the Internet and any computer disk, must ensure the files and disks are scanned with the District's current virus detection software before installation and execution.

   - Employees may use information technology, including the Internet, 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, and other devices constitutes the employee's acceptance of this policy and its requirements.

3. Prohibited Uses

   Prohibited uses include, but are not limited to, the following:

- Sending, receiving, or storing messages 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 armed forces or National Guard.
- Sending, receiving, or storing chain letters.
- Subscriptions to newsletters, advertising, "clubs," or other periodic e-mail which is not necessary for the performance of the employee's assigned duties.
- Engaging in political activities including, but not limited to, solicitation or fund raising.
- Engaging in religious activities including, but not limited to, proselytizing or soliciting contributions.
- Conducting outside employment in any manner.
- Engaging in illegal, fraudulent, defamatory, or malicious conduct.
- Writing or participating in blogs that injure, disparage, and/or defame the employer, members of the public, and/or its employees' reputations by name or implication.
- Downloading, uploading, or otherwise transmitting without authorization
    a) Confidential, proprietary information, or material
    b) Copyrighted material
    c) Illegal information or material
    d) Sexually explicit material
- Obtaining unauthorized access to other systems.
- Using another person's password or account number without explicit authorization by the District.
- Improperly accessing, reading, copying, misappropriating, altering, misusing, or intentionally destroying the information/files of other users.
- Loading unauthorized software or software not purchased or licensed by the District.
- 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.
- Using the District's information technology for personal, non-business purposes in other than a very limited or incidental way.