LYON COUNTY SCHOOL DISTRICT

BOARD POLICY EDB

INTERNET AND PUBLIC NETWORK ACCEPTABLE USE

INTERNET SAFETY

Access to the Internet and public networks through the Lyon County School District network and Internet connection shall be for the purpose of facilitating the acquisition and exchange of information in support of achieving school district educational objectives and accessing the best available research on student learning and K-12 curricula. The Internet is both an invaluable gateway to educationally important information and a source of potentially harmful information to minors. Use by school district employees and students must be responsible and in concert with federal and state law, the acceptable use policies of public access networks, and school district policies, administrative regulations and procedures. Internet safety and responsible use will be fostered through the implementation of regulations and procedures that will include technology protection measures and the monitoring and supervision of users. Internet and public network access through the school district is a privilege that may be revoked by the school district at any time for behavior and actions contrary to this policy and regulation.

1. Internet Safety, Technology Protection Measures and Monitoring of Internet Use

The Children's Internet Protection Act (CIPA) requires technology measures and monitoring be used to discourage and prevent online access to harmful and inappropriate Internet sites. Technology protection measures mean a specific technology, continuously employed on school district Internet equipment and systems, that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.

The district will with "*Best Effort*" practices, protect children and others from depictions that are obscene, child pornography, and harmful to minors; and that promote violence, intolerance, illegal drugs, militant extremism, and the sale, consumption or production of alcoholic and tobacco products. District teachers and staff shall monitor student use of the Internet. The district will employ technology protection and monitoring measures.

a. Definitions:

1) Obscene – Any material or performance when considered as a whole, predominantly appeals to a prurient interest in sex; or that depicts or describes in a patently offensive manner actual or simulated sexual acts, sexual contact, nudity, sadism~~,~~ masochism, excretion or lewd exhibition of the genitals; and that lacks serious literary, artistic, political or scientific value.

2) Child Pornography – Any visual depiction that involves the use of a minor engaging in sexually explicit conduct; or where a depiction appears to be a minor or has been created, adapted or modified to appear that a minor is engaging in such conduct; or is advertised, promoted, presented, described or distributed in a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

3) Harmful to Minors – Any picture, image or graphic image file, or other visual depiction that taken as a whole, and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. A minor is an individual who has not attained the age of 18.

4) Violence – Depictions of extreme cruelty that are intended to hurt or inflict pain.

5) Intolerance – Depictions that advocate prejudice or discrimination against any race, color, national origin, creed, age, religious preference, particular disability or handicap, gender, sexual orientation, or gender identity or preference.

6) Illegal Drugs – Depictions that advocate the illegal use of drugs.

7) Militant Extremism – Depictions advocating extremely aggressive, violent or combative behaviors that advocate violence as a means of achieving ends. This includes information about weapon making, ammunition making, and the making of explosive devices for unlawful purposes.

8) Alcohol and Tobacco Products – Depictions and the promotion of the sale, consumption, or production of alcoholic beverages or tobacco products to minors.

b. Purposes of the Technology Protection Measures and Monitoring:

1) Prevent minor access to inappropriate matter on the Internet and the World Wide Web.

2) Ensure the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

3) Prevent unauthorized access, including so-called "hacking", and other unlawful activities by minors.

4) Prevent the unauthorized disclosure, use, and dissemination of personal information regarding minors.

5) Prevent minors' access to materials that are harmful to themselves.

c. Technology protection measures may be disabled, for adult use, for approved research or other lawful purpose.

2. Right of Privacy on the School District and Public Networks Accessed Through the School District

There is no right to or expectation of privacy for information placed or received on the school district and public networks accessed through the school district's access. The school district reserves the right to access information or materials students and staff store on these networks and remove it when it violates federal or state law, the acceptable use policies of public access networks, or school district policies, administrative regulations and procedures.

3. Disclaimers

a. The district is not responsible for the improper use of public networks by students or staff.

b. Students and staff are responsible for information they place on public networks accessed through the school district network as well as for information they find or take from public networks. Additionally, they are responsible for determining if the information they find or place on public networks is appropriate for use in a school setting.

c. The district is not responsible for information or services that are placed on public networks that may be objectionable to users of the network.

d. The district is not responsible for damage that may occur from student or staff use of public networks including the loss of computer data, damage to computer data, computer viruses that may be acquired from a public network or damages those viruses may cause.

4. Staff and Student Internet Acceptable Use Agreements

The district shall maintain a Staff and Student Internet Acceptable Use Administrative Regulation (AUAR). All staff and students will execute their respective AUAR within the first thirty (30) days of their start date. Students will execute their agreement, signed by a parent, annually. Staff will execute their agreement when hired or when first requiring access to the Internet and shall be provided access to a copy of this and other school district policies and procedures.

5. Educating Students about Appropriate Online Behavior

The district will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber-bullying awareness and response, will develop suitable methods and materials for this purpose.

Legal Reference(s): Children's Internet Protection Act, 20 USC 6801 and 47 USC 254(h) and (l)); regulations at 47 CFR Part 54; NRS 201.235: Obscenity; NRS 393.160: School Property

Policy EDB

Revised 11/16/21