BOARD OF TRUSTEES
CHURCHILL COUNTY SCHOOL DISTRICT

ELECTRONIC RESOURCES AND INTERNET SAFETY

The Electronic Resources and Internet Safety policy of the Board of Trustees supports and promotes positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

NETWORK

The District network includes wired and wireless computers and peripheral equipment, files and storage, and e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the District.

Acceptable network use by District students and staff includes:

- Creation of files, projects, videos, web pages, and podcasts using network resources in support of educational research;
- All posted materials that must follow the Publication Guidelines on page 4;
- Participation in blogs, wikis, bulletin boards, social networking sites, and groups, and the creation of content for podcasts, e-mail, and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum related materials, and student work. Sources outside the classroom or school must be cited appropriately;
- The use of the network for incidental personal use in accordance with all District policies and guidelines; and
- Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use by District students and staff includes but is not limited to:

- Personal gain, commercial solicitation, and compensation of any kind;
- Activity resulting in liability or cost incurred to the District;
- Downloading, installation, and use of games or other applications (including shareware or freeware) without permission or approval from the Director of Technology;
- Support or opposition for ballot measures, candidates, and any other political activity;
- Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
- Unauthorized access to other District computers, networks, and information systems;
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes, and remarks;
- Accessing, uploading, downloading, storage, and distribution of obscene, pornographic, or sexually explicit material; and
- Attaching unauthorized equipment to the District network. Any such equipment will be confiscated and destroyed.

The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, service interruptions caused by its own negligence, or any other errors or omissions. The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's computer network or the Internet.

INTERNET SAFETY

Personal Information and Inappropriate Content*:*

- Students and staff should not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, wikis, e-mail, or as content on any other electronic medium;

- Students and staff should not reveal personal information about another individual on any electronic medium;

- Student pictures or names can be published on any class, school, or District web site unless an opt-out form has been signed and returned to the principal; and

- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

FILTER AND MONITORING

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, even though monitors put forth their best effort, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;

- Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited: proxies, VPN tunnels, https, special ports, modifications to District browser settings, and any other techniques designed to evade filtering or enable the publication of inappropriate content;

- E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District e-mail boxes;

- The District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to District computers;

- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the District; and

- Staff must become familiar with the Internet and monitor, instruct, and assist effectively.

PUBLICATION GUIDELINES

All posted materials must follow the following guidelines:

- Published documents or video conferences may not include a child's phone number, street address or box number, or names (other than first names) of family members;
- Documents or videoconferences may not contain objectionable material or point directly or indirectly to objectionable material; and
- Documents must conform to school board policies and established school guidelines.

COPYRIGHT

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

NETWORK SECURITY AND PRIVACY

Passwords are the first level of security for user accounts. System logins and accounts are to be used only by the authorized owner of the account for authorized District purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- Keep account passwords in a secure location;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen or log off if leaving the computer.

STUDENT DATA IS CONFIDENTIAL

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

NO EXPECTATION OF PRIVACY

The District provides the network system, e-mail, and Internet access as a tool for education and research in support of the District's mission. The District reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders, and electronic communications;
- E-mail;
- Internet access; and
- Any and all data transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Nevada.

ARCHIVE AND BACKUP

Backup is made of all District e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up regularly. Refer to the District retention policy for specific records retention requirements.

DISCIPLINARY ACTION

All users of the District's electronic resources are required to comply with the District's policy and procedures. Violation of any of the conditions of use explained in the Churchill County School District Internet Access Agreement, Electronic Resources and Internet Safety policy, or in these procedures could be cause for disciplinary action, including suspension or expulsion from school, and suspension or revocation of network and computer access privileges.

ADOPTED: 01/11/17
REVIEWED:
REVISED:
REVIEW RESPONSIBILITY: Board of Trustees / Superintendent