Computer Education – Assisted Instruction Internet Safety IGAO

It is the policy of Crook County School District #1, that to the extent reasonably possible, staff and students will be encouraged and permitted to utilize the computer network provided by CCSD#1 for the purpose of facilitating learning and providing the best educational experience possible for its students. In this regard, CCSD#1 has made available to students and staff, electronic mail and the Internet. To gain access to email and the Internet, all students under the age of eighteen (18) must obtain parental permission and sign and return a parental permission form to the school district. Students eighteen (18) and over may sign their own forms. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. While it is possible for students to access inappropriate material and otherwise misuse the system, it is the intent of CCSD#1 that Internet access should only be used to further the educational goals and objectives set out for each student. It is the policy of this school district to try to educate our students using modern technology which the students will need to be familiar with in order to be successful in their subsequent careers. However, in order to utilize this modern technology, it will ultimately be the responsibility of parents and guardians of minors to set and convey standards to their children which they will follow while utilizing this technology. To that end, CCSD#1 will support and respect each family's right to decide whether or not to apply for access.

District Internet and Email Rules

Students are responsible for good behavior on school computer network, just as they are in the classroom or a school hallway. Communicating on the network is often public in nature. General school rules for behavior and communications apply.

Internet filters shall be used to block access to obscenity, child pornography, and materials deemed harmful to minors. Disciplinary action shall be taken against any student who tampers with the filters. The filters may only be disabled for bona fide research or other lawful purposes, and may only be disabled by a CCSD#1 designated representative.

Internet Safety Training

In compliance with the Children's Internet Protection Act, each year all CCSD#1 students will receive Internet safety training which 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.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parental permission is required. Access is a privilege, not a right. Access entails responsibility. Individual users of CCSD#1 computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with district standards and will honor the agreements they have signed. Beyond the clarification of such standards, CCSD#1 is not responsible for restricting, monitoring, or controlling the communications of individuals using the network.

Network storage areas are not to be considered private or personal property of students or staff. They are learning areas subject to review by administrators and

teaching staff. Any files and communications may be reviewed by the administration or staff to maintain system integrity and to ensure that users are using the system responsibly. Users should not expect that files stored on district servers will be private.

While school teachers of younger students will generally guide them toward appropriate materials, older students and students utilizing the system outside of regular school hours will need to be directed by families in the same manner they direct their children's use of television, telephones, movies, radio, and other potentially offensive media.

The following conduct and utilization of the Internet by students and staff are **NOT permitted**.

1. Sending or displaying offensive messages or pictures,
2. Using abusive, objectionable or obscene language,
3. Searching for, downloading, or otherwise reviewing any type of sexually explicit, obscene material or other information,
4. Harassing, insulting or attacking others,
5. Damaging computers, computer systems, or computer networks,
6. Violating copyright laws or otherwise using the network for any illegal purpose,
7. User shall not use or attempt to discover another user's password nor shall user use or let others use another person's name, address, passwords, or files for any reason, except as may be necessary for legitimate communication purposes and with permission of the other person,
8. Trespassing in another's folders, work or files,
9. Intentionally wasting limited resources,
10. Employing the network for commercial purposes,
11. Otherwise accessing forums or "chat rooms" devoid of educational purpose;
12. User shall not tamper with computers, networks, printers, or other associated equipment or software without the express permission of supervising staff
13. User shall not write, produce, generate copy, propagate or attempt to introduce any computer code designated to self-replicate, damage or otherwise hinder the performance of any computer's memory, file system or software.
14. Student using school district computers and/or accessing school district web pages, or using the Internet service provided by the school district, shall not engage in hacking and shall not access unauthorized sites or participate in any other unlawful activities online.
15. Disclose, use or disseminate personal identification information regarding students or staff.

Supervision and Monitoring

It shall be the responsibility of all district employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling, filtering or otherwise modifying of any technology protection measures shall be the responsibility of a designated representative.

To make a request:

1. Email the CCSD#1 technology department; or
2. Submit a request, whether anonymous or otherwise, to the superintendent or the superintendent's designee.
3. Requests for access shall be granted or denied within three (3) school days, if a request was submitted anonymously, persons should either attempt to access

the web site requested after three (3) school days or log back in to see the status of the request.

4. Appeal of the decision to grant or deny access to a web site may be made in writing to the CCSD#1 Board of Trustees. Persons who wish to remain anonymous may mail an anonymous request for review to the CCSD#1 Board of Trustees at the central office, stating the web site that they would like to access and providing any additional detail the person wishes to disclose.
5. In case of an appeal, the Board of Education will review the contested material and make a determination.
6. Material subject to the complaint will not be unblocked pending this review process.

In the event that a CCSD#1 student or employee feels that a web site or web content that is available to students through district Internet access is obscene, child pornography, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for students, the process described above should be followed, except any decision to filter or block web content will be made within thirty (30) days.

Penalty

Violations will result in a loss of access as well as other disciplinary or legal action. The first offense will generally result in a warning and loss of computer privileges/Internet access until a parent conference, and further loss of privilege for such time as is determined by the administration. A second offense or a first offense of a flagrant nature, such as using the system for illegal behavior or intentionally damaging school district hardware or software, may result in removal from a class, termination of computer/network privileges, or recommendations for suspension and/or expulsion.

Revised: September 19, 2002
Revised: June 17, 2013
Revised: February 20, 2018