District Internet Safety Plan

The District provides Internet access to its employees, Board members, and students for educational purposes only. The District's Internet system has not been established as a public access service or a public forum. The District has the right to place restrictions on use to ensure that use of the system is in accord with its limited educational purpose.

Student use of the District's Internet system will be governed by this document, the District's Acceptable Use Policy (see below), related District and school regulations, and the student disciplinary code. Staff use will be governed by this document, related District policies and regulations, and District employment policy. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the District Internet system. Because the law considers information and material on the school network as public documents and requires the monitoring of Internet activity, users should have limited to no privacy expectations regarding the contents of their personal files and records of their online activity while on the District system.

The District Internet system is a limited public forum. The District may restrict access to materials or may place restrictions on student speech for valid educational reasons.

This document was developed in accordance with the statutory requirements of the Children's Internet Protection Act (CIPA).

The District promotes the effective, educational use of the Internet in school through professional development. Student and staff users of the District Internet system are being educated regularly regarding the safe, ethical, legal, and responsible use of the Internet and of the District's Internet system and their rights and responsibilities under this plan. Student use and activities will be structured in a manner that is appropriate to the age and skills of students.

The District protects against access to materials that are considered inappropriate for users to access through the District Internet system in the following manner:

1. The District recognizes that Internet resources can be categorized as prohibited, restricted, limited access, or approved material. Prohibited material may not be accessed by the students or staff at any time, for any purpose. Restricted material may be accessed by students in the context of specific learning activities that have been approved by the Superintendent or by the IT Director for professional development purposes. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher. Approved material, on the other hand, can be accessed at all times.

2. The District has implemented the use of a technology protection measure (filtering software), which is a specific technology that will protect against access to visual depictions that are obscene, child pornography, and materials that are harmful to minors, as defined by CIPA. At the discretion of the District or school, the filtering software may also be configured to protect against access to other material considered inappropriate for student access. The District recognizes, however, that filters are not perfect. They block sites that should not be blocked and let through sites that should be blocked. Therefore, Cherokee Community Schools do not rely on filters as a sole protection measure. Education on how to handle accidental access, supervision, parental support of policies and responsible use play important roles.
3. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material, if access to such sites has been inappropriately blocked by the filtering software.
4. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the filtering software.
5. Student use of the District Internet system will be supervised by staff in a manner that is appropriate to the age of the students and circumstances of use.
6. The District has developed procedures to monitor student use of the Internet through an analysis of Internet usage records.
7. The Acceptable Use Policy (see below) includes provisions that address the following safe and responsible use issues:

- Access to inappropriate material.
- Privacy and communication safety standards for self and others
- Illegal activities, including computer security violations, actions taken to disrupt the performance of a computer system, and the use of the Internet to engage in other criminal acts.
- Inappropriate language.
- Plagiarism and copyright infringement.
- Actions or use that may disrupt or jeopardize the security or effective performance of the District's network or the Internet.
- Safety and security when using direct electronic communication.

The District follows guidelines for protecting student personal information when accounts are established on third party websites in accordance with CIPA.

The District will protect against the unauthorized disclosure, use, or dissemination of personal or confidential information of students in accordance with state, federal and local regulations.

The District will develop regulations addressing the disclosure of student information, posting student-created material, and posting pictures of students on the District website.

Each school year, students and staff must sign an agreement to be allowed access the Internet.

The District educates students to respect intellectual property and observe copyright protection related to material that is accessed through or placed on the Internet.

The District has developed District guidelines to promote the effective educational use of the Internet, protect the privacy rights and other rights of students and staff, limit potential liability of the District for the inappropriate placement of material, and present an image that will reflect well on the District, schools, staff, and students, and adheres to Iowa state law.

The administrative responsibilities of the District administrative staff related to the District Internet system are as follows:

1. The IT Director, or his/her designee, will serve as the coordinator to oversee the District Internet system. The superintendent is also authorized to develop regulations and agreements for the use of the District Internet system that are in accord with this plan, and other District policies.
2. The building principal, or his/her designee, will serve as the building-level coordinators for the District Internet system, and be responsible for interpreting this plan and related regulations at the building level.
3. The District conducts ongoing evaluation of the issues related to this plan, related regulations, and the strategies implemented by schools under this plan.

Acceptable Use Policy

General Information

The Cherokee Community School District provides computer equipment, computer services, and Internet access to its students and staff for educational purposes only. Computers are located in classrooms, pods, and libraries. Students in grades 9-12 are supplied with computer bags to take home their PC's. All others PC's must stay on school property. All online activity is monitored on school issued and owned PC's at ALL times

Cherokee Community School District has established procedures to comply with the Children's Internet Protection Act (CIPA), which mandates that:

- All computers incorporate technology to protect students from obscene material, child pornography, and other harmful material
- Student activity online is monitored
- The District maintains a District Internet Safety Plan (See above).

Although Cherokee Community Schools use filtering software, all parties must be aware that filters are imperfect. Material that should not get through does get through and material that should not be blocked is blocked.

Students or staff who inadvertently access inappropriate material, should notify the supervising teacher or the Technology Department so that the website may be blocked and to avoid any problems if the access is picked up during the monitoring process.

These guidelines are provided so that staff, community, student users, and the parents/guardians of students are aware of their responsibilities. The district may modify these rules at any time.

Information Content and Uses of the System

The user agrees not to publish on or over the system any information, which violates or infringes upon the rights of any other person or any information which would be abusive, profane, or sexually offensive. The user agrees not to use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity that is prohibited by law.

Cherokee Community Schools provide access to the Internet; however, the District and the system administrators have no control over content. The District has taken steps to prevent access to objectionable content, but potential dangers remain. Students and their parents/guardians are advised that some systems may contain objectionable or illegal material. Cherokee Community Schools and the system administrators do not condone the use of such materials and do not permit usage of such materials in the school environment. Knowingly bringing such materials into the school environment may result in disciplinary action. At any time, the systems administrator may prohibit the use of smart phones, or other devices on the district network.

Students may not bring personal Laptops, IPad, Etc. into the district. The district provides a 1:1 PC program where all students are provided a School owned PC.

Standards for Use of Computer Networks

Any individual engaging in the following actions when using computer networks/computers shall be subject to discipline or legal action:

- A. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate federal, state, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the network. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.
- B. Using the computer network(s)/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.
- C. Using the computer network(s) in a manner that:
  - 1. Intentionally disrupts network traffic or crashes the network;
  - 2. Degrades or disrupts equipment or system performance;
  - 3. Uses the computing resources of the school district for commercial purposes, financial gain or fraud;
  - 4. Steals data or other intellectual property;
  - 5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another user;
  - 6. Gains or seeks unauthorized access to resources or entities;
  - 7. Forges electronic mail messages or uses an account owned by others;
  - 8. Invades privacy of others;
  - 9. Posts anonymous messages;
  - 10. Possesses any data which is a violation of this policy; and/or
  - 11. Engages in other activities that do not advance the educational purposes for which computer networks/computers are provided.

Online Safety and Privacy

The Children's Internet Protection Act (CIPA) requires that schools establish a District Internet Safety Plan (see above). It details specific measures that the school is taking to ensure the students' safety while working online. This and other curricular documents are available upon request from the office of the superintendent.

Email

Email messages on the Cherokee Community School District network are the property of the district and may be accessed at any time. Messages received by the system are retained on the system until deleted by the recipient or until they reach the expiration date set by the system administrator.

Cherokee Community School District will provide email accounts to students for curricular/ educational purposes. Business, personal entertainment, or other non-educational uses are to be avoided. Student use of outside email accounts or web-based email is prohibited and a violation of this policy.

A canceled Cherokee Community School District account will not retain email. Users are expected to remove old messages in a timely fashion. The system administrators may remove messages if not attended to regularly by the user.

The Children's Internet Protection Act (CIPA) mandates that student online activity is monitored. District email may be monitored electronically.

It is a violation of this AUP to send email that is defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal. Anyone receiving such email should refer it to the proper authorities for investigation. Cherokee Community School District reserves the right to cooperate fully with local, state, or federal officials in any investigation concerning or relating to any email transmitted on the Southern Regional network.

Security

Security on any computer system is a high priority. If a user identifies a security problem on the system, the user must notify a system administrator. The user should not demonstrate the problem to others. Users should not allow others to use their account and password. Attempts to log in to the system using either another user's account or as a system administrator will result in discipline. Users should immediately notify a system administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any user identified as a security risk will be subject to disciplinary action.

Vandalism

Vandalism will result in the limited use of system privileges and other disciplinary measures in compliance with district policy and the discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or other networks that are connected to the Internet, or intentional damage to hardware or software on the system.

Printing

The printing facilities of the Cherokee Community School District network should be used judiciously. Unnecessary printing is a drain of the capacity of the networks, adds expense, and shortens the life of the equipment.

Privately Owned Technology Devices

Privately owned technology device refers to any technology hardware or software that is borrowed, purchased, owned and/or maintained by the pupil or staff member at no expense to the school or district.

Privately owned technology devices include any type of computer, wireless phone, electronic reader, tablet, video recording device or camera.

The school district shall assume no responsibility for the security or damage to any privately owned technology device brought to school.

Students may ***not*** use privately owned technology devices accept wireless phones at the discretion of administration, or teachers. Teachers who wish to allow the use of privately owned technology devices shall notify their immediate supervisor as to the nature of this use.

Any staff member who uses a privately owned technology device while in school for any purpose must comply with all district policies and regulations. The school district assumes no responsibility for any privately owned technology device or software brought to school by a student or staff member.

Violations

Individuals violating this policy shall be subject to consequences that include but are not limited to the following:

- Use of the network only under direct supervision;
- Suspension of network privileges;
- Revocation of network privileges;
- Suspension of computer privileges;
- Revocation of computer privileges;
- Suspension from school;
- Expulsion from school; and/or
- Legal action and prosecution by the authorities.

_____ _____

IT Director Date Super intendant Date

Revision 100.2 4/23/2024