# Center Point ISD

## Electronic Information System/Network User Policy

## Staff/Adult

## 2021-2022

## Acceptable Use Policy

## Section I

## CENTER POINT INDEPENDENT SCHOOL DISTRICT

## Electronic Information Systems/Network User Policy

### Introduction

Center Point ISD recognizes the need to regulate the acceptable use of technology to control the use of the Internet. The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. The District recognizes that the Internet can be used to facilitate many educational activities. The Internet is not meant to replace education, but rather, to facilitate the educational process. It should be used as an adjunct to teaching. The Internet can be a valuable learning tool in the areas of electronic mail, research, data searches, enrichment materials, electronic field trips, and library references. Center Point ISD resources available on the Internet will allow classroom projects such as pen pal discussions, scientific data collection, and international cultural exchanges. News retrieval services, encyclopedias, scientific and educational databases will be instantaneously accessible to Center Point students and teachers.

### Philosophy

Center Point ISD believes in the value of incorporating learner-centered experiences in the total educational process. Our philosophy is to make Network/Internet access available to all students, teachers, and staff in Center Point ISD. Therefore, the District has made Internet-access available to all grade levels because of the many resources it has to offer and the enhanced opportunities for research it provides.

### Educational Value Risk

With this access comes the availability of material that may not be considered to be of educational value in the context of the school setting. Sites accessible via the Network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Although the District will attempt to limit access to most of this objectionable material, controlling all materials on the Network/Internet is impossible. On a global network, it is impossible to control all materials; an industrious user may discover controversial information. The Center Point ISD Board of Trustees believes that the valuable information and interaction available on these networks far outweigh the possibility that users may locate material that is not consistent with the educational goals of Center Point School District.

**Internet Safety**

It is the policy of Center Point ISD to:

a. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, chat rooms, social media websites, and other forms of direct electronic communications;

b. Prevent unauthorized access and other unlawful online activity

c. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors;

d. Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC254(h)].

**Access to Inappropriate Material**

To the extent practical, technology protection measures, or "Internet filters", shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act (CIPA), blocking shall be applied to visual depiction of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

**Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of Center Point ISD online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes;

a. Unauthorized access, including so-called 'hacking' and other unlawful activities; and

b. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

**Education, Supervision and Monitoring**

It shall be the responsibility of all members of Center Point ISD staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act.

The Campus Principals or designated representatives will provide age-appropriate training for students who use the Center Point ISD Internet facilities. The training provided will be designed to promote the Center Point ISD commitment to:

a. The standards and acceptable use of Internet services as set forth in the Center Point ISD Internet Safety Policy; b. Student safety with regard to:

1. Safety on the Internet;

2. Appropriate behavior while online, on social networking Websites, and in chat rooms; and

3. Cyberbullying awareness and response.

c. Compliance with the E-rate requirements of the Children’s Internet Protection Act (“CIPA”)

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District’s acceptable use policies.

**Network and Internet Use**

**User Responsibilities**

Network/Internet users are responsible for their actions in accessing available resources which are consistent with the educational goals of Center Point ISD.

**Levels of Access/Teacher Supervision**

All students are expected to exercise responsible use of the Network/Internet at all times. Elementary students will have a teacher/aide monitoring their work on the Network/Internet. At middle school, and high school, it is the intent of the district to have personnel present during the students' Network/Internet use; however, due to the nature of their work, it may not always be possible to directly monitor their work. Sites being accessed by users may be monitored at any time.

Access to the District's electronic communications system will be governed as follows:

1. With the approval of the immediate supervisor, District employees will be granted access to the District's system.

2. The District will require that all passwords be changed periodically at the discretion of the Technology Director or designee.

3. Any system user identified as a security risk or having violated District and/or campus computer-use guidelines may be denied access to the District's system.

**Acceptable Use**

Network/Internet access shall be used to improve learning and teaching consistent with the educational goals of Center Point ISD. The District expects legal, ethical and acceptable use of the Network/Internet. Acceptable use will be defined by district policy and local campus administration guidelines. 5

**Unacceptable Use**

Every Center Point ISD user has the responsibility to respect and protect the rights of every user in our community and on the Internet in accordance with the laws of Texas and the United States and with rules and guidelines as set by district policy. All users should be aware that the unacceptable use of electronic information resources can be a violation of local, state, and federal laws. Violations can lead to prosecution. Students are expected to use moral and ethical guidelines in making value decisions regarding network use. Using the network is a privilege, not a right, and the privilege may be revoked at any time for unacceptable conduct. The campus principal will make the final determination as to what constitutes unacceptable conduct.

Unacceptable conduct includes, but is not limited to, knowingly engaging in any of the following:

- Any use that is illegal or in violation of other board policies, including harassing, cyberbullying, discriminatory or threatening communications and behavior; violations of copyright laws, etc.;
- Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;
- Any inappropriate communications with students or minors;
- Any use for private financial gain, or commercial, advertising or solicitation purposes;
- Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit.
- No employee shall knowingly provide school email addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the campus principal or other appropriate administrator.
- Any communication that represents personal views as those of the District or that could be misinterpreted as such;
- Downloading or loading software or applications without permission from the system administrator;

- Opening or forwarding any e-mail attachments (executable, batch, and/or script files) from unknown sources and/or that may contain viruses or malicious software;
- Sending mass emails to District users or outside parties for school or non-school purposes without the permission of the system administrator (or other designated administrator).
- Any malicious use or disruption of the District's computers, networks, and Internet services or breach of security features;
- Any misuse or damage to the District's computer equipment;
- Misuse of the computer passwords or accounts (employees, students, or other users);
- Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct, including the use of profanity or vulgar, obscene or sexually explicit language;
- Any attempt to access inappropriate/unauthorized sites (i.e. Internet/Websites, intranet websites, and/or application servers);
- Failing to report a known breach of computer security to the system administrator;
- Executing, using, or viewing any application or website that is resource intensive, resulting in excessive network saturation and denial-of-service for other users;
- *Users* using District computer networks are prohibited from gaining unauthorized access to any information system or network to which they have not been expressly granted access. *Users* using District computer networks are also prohibited from in any way damaging, disrupting, or interfering with the operations of multi-user information systems to which they are connected. Likewise, *users* are prohibited from capturing or otherwise being in possession of passwords, encryption keys, or any other access control mechanism that has not been expressly assigned to them. *Users* are furthermore prohibited from possessing or using software tools which could provide unauthorized access to system resources (these include password dictionary attack programs, encryption key brute-force discovery programs, and software for defeating copy-protection mechanisms).
- Using school computers, networks, and Internet services after such access has been denied or revoked;
- Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates these rules;
- Use that violates this Policy, the student code of conduct or the employee standards of conduct;
- Unauthorized disclosure, use, or distribution of personally identifiable information or personal identification regarding students or employees;
- Personal or political use to advocate for or against a candidate, office-holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit;
- Participating in chat rooms other than those approved, sponsored and/or overseen by the District; and/or
- The use of personal devices such as PDA's (Palms, Visors, cell phones, with web capability, etc.) and laptops, iPads (either wireless or Ethernet) or any device used to access CPISD Networks is prohibited unless Policy provides otherwise.

## INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

## ONLINE CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.

3. System users may not use another person’s system account without written permission from the District Administrator or District Technology Director, as appropriate.

4. System users must purge electronic mail in accordance with established retention guidelines.

5. System users may redistribute copyrighted programs or data only with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

6. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

7. The signatures on this document are legally binding and indicate that those who signed have read the terms and conditions carefully and understand their significance.

## VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

## FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

## INFORMATION CONTENT/THIRD PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school’s electronic environment will be subject to disciplinary action in accordance with District policies.

## DISTRICT WEBSITE

The District will maintain a District Website for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated Webmaster. The Technology Director and the District Webmaster will establish guidelines for the development and format of Web pages controlled by the District.

No commercial advertising will be permitted on a Web site controlled by the District.

## TEACHER AND EXTRA-CURRICULAR WEB PAGES

With the approval of the campus principal, teachers and extracurricular organizations may establish Web pages linked to a campus or district website; however, all material presented on the Web page must relate specifically to organization activities.

## PERSONAL WEB PAGES

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.

## TERMINATION/REVOCATION OF SYSTEM USER ACCOUNT

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the principal or District Technology Director receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

**DISCLAIMER**

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

**Acceptable Use Policy**

**Section II**

**Agreement**

**EMPLOYEE/GUEST AGREEMENT**

I have read the District's electronic communications system policy and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system; and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

Signature

Date

Printed Name ______________________________________________________