Collinsville Independent School District
Acceptable Use Policy
Acceptable Use Policy
Guidelines on the Acceptable Use of Electronic Information
Resources:

Information resources offer access to computers and people throughout the world. Students and staff will have access to electronic mail and college and university libraries, information and news from a variety of sources and research institutions, software of all types, and discussion groups on a wide variety of topics, and much more!

While the emphasis here is on appropriate use, there is no intent to diminish the vital nature of electronic information services. The concerns described here are real, but they should not discourage school officials from planning for the appropriate use of one of education's newest and most valuable tools.

While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or unethical purposes avenues for reaching students, teachers, and others, including parents. The following represent some of the inappropriate uses that may occur:

• using the network for commercial advertising
• using copyrighted material in reports without permission or proper citation credit
• using the network to lobby for votes
• using the network to access a file that contains pornographic pictures, taking them home, and telling parents, "I got them at school"
• using the network to send/receive messages that are racist
• using the network to send/receive inflammatory messages
• creating a computer virus and/or placing it on the network
• using the network to send/receive a message with someone else's name on it
• using the network to send/receive a message that is inconsistent with the school's code of conduct
• using the network to send/receive messages that are sexist and contain obscenities
• using the network to provide addresses or other personal information that others may use inappropriately
• using the network for sending and receiving a large number of personal messages
• using the network to bully others

All users should be aware that the inappropriate use of electronic information resources can be a violation of local, state, and federal laws.

Violations can lead to prosecution.

User Contract:

Electronic Information Resource Contract

We are pleased to announce that electronic information services are available to students and teachers in our district. The Collinsville Independent School District strongly believes in the educational value of such electronic services and recognizes the potential of such to support our curriculum and student learning in our district.

Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Collinsville Independent School District will make every effort to protect students and teachers from any misuses or abuses as a result of their experiences with an information service. All users must be continuously on guard to avoid inappropriate and illegal interaction with the information service.

Please read this document carefully. When signed by you and, if appropriate, your guardian/parent, it becomes a legally binding contract. We must have your initials where indicated and your signature and that of your guardian/parent (if you are under 18) before we can provide you with an computer access account.

Listed below are the provisions of this contract. If any user violates these provisions, access to the information service may be denied and you may be subject to disciplinary action.

Terms and Conditions of This Contract

I. Personal Responsibility

As a representative of this school, I will accept personal responsibility for reporting any misuse of the network to the system administrator. Misuse can come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described below. All the rules of conduct described in the District publication entitled Student Handbook apply when you are on the network.

II. Acceptable Use

The use of my assigned account must be in support of education and research and with the educational goals and objectives of the Collinsville Independent School District (these may be found in the District document entitled Student Handbook). I am personally responsible for this provision at all times when using the electronic information service.

Use of other organization's networks or computing resources must comply with rules appropriate to that network. Transmission of any material in violation of any United States or other state organizations is prohibited.

This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.

Use of commercial activities by for-profit institutions is generally not acceptable.

Use of product advertisement or political lobbying is also prohibited. I am aware that the inappropriate use of electronic information resources can be a violation of local, state and federal laws and that I can be prosecuted for violating those laws.

Hacking, using file sharing programs (Kazaa, WinMX, bit torrent) or installing any software is prohibited.

Anyone who has an .exe file (or executable program) in their folder or on a disk brought in from outside the district will be in violation.

Use of non-school issued email on a school owned computer or device.

III. Privileges

The use of the information system is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Each person who receives an account will participate in an orientation or training course with a high school or elementary faculty member as to proper behavior and use of the network. The district's LAN/system administrator (operating under the aegis of the school board and the district office) will decide what is appropriate use and their decision is final. The system administrator(s) may close an account at any time deemed necessary. The administration, staff, or faculty of Collinsville Independent School District may request that the system administrator deny, revoke, or suspend specific user accounts.

IV. Network Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These rules include (but are not limited to) the following:

• Be polite:
Never send, or encourage others to send, abusive messages.

• Use appropriate language:

Remember that you are a representative of our school and district on a non-private system. You may be alone with your computer, but what you say and do can be viewed globally! Never swear, use vulgarities, or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

• Privacy:

Do not reveal your home address or personal phone number or the addresses and phone numbers of students or colleagues.

• Electronic Mail:
Electronic mail (e- mail) is not private. Messages relating to or in support of illegal activities must be reported to the authorities.

• Disruptions:

Do not use the network in any way that would disrupt use of the network by others.
Other Considerations:

• Do be brief. Fewer people will bother to read a long message.
• Do minimize spelling errors and make sure your message is easy to understand and read.
• Do use accurate and descriptive titles for your articles.
• Do tell people what it is about before they read it.
• Do get the most appropriate audience for your message, not the widest.
• Do remember that humor and satire is very often misinterpreted.
• Do remember that if you post to multiple groups, specify all groups in a single message.
• Do cite references for any facts you present.
• Do forgive the spelling and grammar errors of others.
• Do keep signatures brief.
• Do remember that all network users are human beings. Don't "attack" correspondents; persuade them with facts.
• Do post only to groups, resources, and sites approved by CISD.

V. Services

The Collinsville Independent School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. Collinsville Independent School District will not be responsible for any damages suffered while on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the information system is at your own risk. Collinsville Independent School District specifically disclaims any responsibility for the accuracy of information obtained through its services.

VI. Security

Security on any computer system is a high priority because there are so many users. If you identify a security problem, notify the system administrator at once. Never demonstrate the problem to other users. Never use another individual's account without written permission from that person. All use of the system must be under your own account. Any user identified as a security risk will be denied access to the information system.

VII. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses. Any vandalism will result in the loss of computer services, disciplinary action, and legal referral.

VIII. Updating

The information service may occasionally require new registration and account information from you to continue the service. You must notify the information system of any changes in your account information.

District Web Publishing Guidelines

Educational Value - Material to be published must not display, access, or link to sites deemed offensive. All published material must have educational value or support the district guidelines, goals and policies.

Publishing

Only materials authorized and reviewed by a teacher or administrator will be published. Student work may only be published on a teacher's web page, district approved site, or social media site used by the district by a teacher or by the technology director and then only when appropriate. Students may not publish work directly to a school web site.

Protect Privacy

At no time shall any student's personal information (home address, e- mail address, or phone number) appear on CISD Internet/Intranet published materials. All contact information should identify the content sponsor or teacher.

Student Safety

To assure student safety, a student's picture and full name shall not appear on the same page. A stranger should never be able to connect a student's name with a face. Student projects, achievements, photos of and by, sports statistics, sports photos and school activity photos and video, honor rolls, and other related items may be placed on the school website, or social networking sites maintained by district employees to promote the school district and its activities.

Copyright Laws

Adhere to all copyright laws.

Content Monitoring/Auditing

CISD Administration reserves the right to audit and/or adjust materials and/or activity on any Internet/Intranet Server publishing content sponsored by a CISD organization.

Site Guidelines

Active Links
The web is a very dynamic resource. It is strongly recommended that links to external existing sites be checked regularly to insure that CISD sponsored links are not going to sites that do not meet CISD's Acceptable Use Agreement.

Current Files
Only active files that are required for the proper operation of the Internet/Intranet Site should be stored on the Internet/Intranet Server.

File Size
Due to limited storage space and varying network speeds, it is recommended that file sizes should be kept as small as possible. In rare cases, where larger file sizes are required, please inform users by making a note on referring documents.

Advertising
Individuals are not to use CISD web resources for personal gain or profit. Accordingly, there is no advertising, sale or solicitations by individuals on CISD sponsored sites.

Navigational Links
It is suggested that each page contain clear links to the sponsoring site's home page and/or higher- level pages. There should always be navigational clues to help users find their way.

Contact Information
Out of courtesy to Internet/Intranet users, each page shall contain contact information for the content sponsor.

Appearance
Sites will strive to maintain a tight integration with the rest of the district site which includes the use of appropriate school colors and logos.

Collinsville ISD Internet Safety Plan
1. The district is providing Internet access to its employees, staff, and students. The district's Internet system has a limited educational purpose. 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.

2. Student use of the district's Internet system will be governed by this document, the district's Acceptable Use Policy (AUP), related district and school regulations, and the student disciplinary code. Staff use will be governed by this document, related district policies and regulations, district employment policy.
Internet system:

1. Users should have limited privacy expectations regarding the contents of their personal files and records of their online activity while on the district system.

2. The district may restrict access to materials for valid educational reasons.

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

a. The district promotes the effective, educational use of the Internet in school through professional development and the establishment of a district web site.

b. Student and staff users of the district Internet system have been informed regarding the safe, ethical, legal, and responsible use of the Internet and of the district's Internet system and their responsibilities under this plan.

c. Student use and activities will be structured in a manner that is appropriate to the age and skills of students.

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

i. 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 a teacher or by staff 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.

ii. 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, CISD does not rely on filters as a sole protection measure.

iii. 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.

iv. 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.

v. 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.

vi. The district has developed procedures to monitor student use of the Internet.

vii. The AUP includes provisions that address the following safe and responsible use issues:

1. Access to inappropriate material.

2. Privacy and communication safety standards for self and others

3. 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.

4. Inappropriate language.

5. Plagiarism and copyright infringement.

6. Actions or use that may disrupt or jeopardize the security or effective performance of the district's network or the Internet.

7. Safety and security when using direct electronic communication

8. 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.

9. The district has developed guidelines for addressing the disclosure of student information, posting student created material, and posting pictures of students on the district web site (see web publishing procedure)

10. Each school year, parents/guardians must sign an agreement to allow their child to access the Internet.

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

12. The district has developed district web site guidelines to promote the effective educational use of the Internet, protect the privacy rights and other rights of students and staff, placement of material, and present an image that will reflect well on the district, schools, staff, and students.

13. The administrative responsibilities of the district administrative staff related to the

district Internet system are as follows:

a. The superintendent, or his/her designee, will serve as the coordinator to oversee the district Internet system. The superintendent is 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.

b. The building administrator, 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.

c. The district conducts ongoing evaluation of the issues related to this plan, related regulations, and the strategies implemented by schools under this plan.

BYOD

(Bring Your Own Device)
Student, Teacher and Parent Guide

PURPOSE

Collinsville ISD is committed to moving students and staff forward in a 21st century learning environment. As part of this plan, CISD will now allow students and staff to access the PirateNet wireless network using their own technology devices (laptops, Smart Phones, iPads etc.) during the learning day. With classroom teacher approval, students may use their own devices in the classroom to access and save information from the Internet, communicate with other learners and use the productivity tools loaded on their devices.

PLAN

Beginning Spring 2012, students may bring their own technology devices to school. Users will be prompted to accept the following terms of use prior to each attempt at connecting to the PirateNet network:

CISD is providing wireless connectivity as a guest service and offers no guarantees that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of the CISD wireless network is entirely at the risk of the user, and Collinsville ISD is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury or damages resulting from the use of the wireless connection. All users of the Collinsville ISD network are bound by the district's Acceptable Guidelines for Technology. By entering, "Accept" below, you are agreeing to all of the above cautions and policies as they pertain to non-district devices.

Students and staff who do not accept the terms of service will not be able to access the CISD Network. The terms of service prompt will post each time an outside user attempts to use this network. Once on the PirateNet network, all users will have filtered Internet access just as they would on a district owned device.

FREQUENTLY ASKED QUESTIONS
STUDENTS:

I have my laptop with me in class. How do I get on the Internet now?

Answer: Most laptops or other personal devices (smart phones) will detect a wireless connection when you are near one (wireless must be turned on). Most of the time your technology tool will ask you if you would like to join the network. When prompted, choose **PirateNet** from the list. Once you choose this network, you will be prompted to accept the terms of service. Read this carefully so that you know what should be expected. You may also be prompted to enter your login name and password (same as you use for CISD network access).

My laptop is not prompting me to choose a wireless network. Is there another way to connect?

Answer: In the settings menu of your device, there is usually an icon for a network. Go to this icon and choose the **PirateNet** from the list or prompt your computer to look for a wireless network. Always consult your device's owner's manual for exact directions for accessing a wireless network.

I just can't get my laptop to connect to the network. Can I get some help from someone?

Answer: Students who cannot access the CISD PirateNet wireless network, or who may have technical issues with their technology tool, need to take care of this issue by working with their user's manual that came with the device (not during class time). These are not CISD devices and the district is not allocating resources at this time to troubleshoot issues.

I brought my iPad to school to use in the classroom, but my teacher said I couldn't use it in her classroom. Can I still use it?

Answer: The ***teacher in the classroom*** has the final say on procedures in the classroom. If he or she asks you not to use your device, then you should follow those directions. Access is only available, not guaranteed for each classroom situation.

Can I use my device to record audio/video?

Answer: Recording others without their permission is not allowed in a school setting. Likewise recording in classes is up to the sole discretion of the teacher or principal. As a general rule devices that have this capability should not be used to record except when directed by a teacher as part of the lesson. Under no circumstances are video/audio recording devices allowed out in bathrooms, locker rooms, or other similar areas.

I need to save my work on a CISD drive. Why can't I access this resource?

Answer: You are on the PirateNet Network. It is not the same as the network you would normally access from a campus computer. You will not see your network drives, so you will need to save your work on your device. The best solution for 7-12 students is to save the work to their locker in gaggle and then use a school computer to go to gaggle and move that work to a network drive.

I need to print the spreadsheet I just created. Why is there no printer listed when I try this?

Answer: Like the shared folders, printers are on the CISD network and will not be available when you login to the guest network. Some printing solutions include: saving it to a flash drive and printing from home or another campus computer. You can also save it to the locker in gaggle and then print it from a school computer. Keep in mind that using campus printers in the classroom or other learning spaces is at the discretion of the teacher or other campus administrators.

My laptop was stolen when I brought it to school. Who should I contact about this?
Answer: Bringing your own technology device to school can be useful; however some risks are involved as well. It is always a good idea to record the device's serial number in case of theft. CISD is not responsible for the theft of a device, nor are we responsible for any damage done to the device while at school. Any time a theft occurs, you should contact the campus principal but under no circumstance is CISD responsible for the device.

Why am I filtered on my own computer/device? Shouldn't I be able to see what I want to on my own tool?

Answer: Student filtering is required by federal law of all public schools. The Children's Internet Protection Act (CIPA) requires all network access to be filtered, regardless of the tool you use to access it while in a public school. Your laptop or phone is the device. The network you are using while at school belongs to CISD and will be filtered.

Am I still held accountable for the Acceptable Use Policy ("AUP") I signed at the beginning of the school year even though this is my own personal computer?

Answer: Yes. The Acceptable Use Policy for CISD remains in effect even when you are using your own laptop, smart phone, iPad etc. Each time you attempt to access the network at school you will be prompted to accept the terms of service which include the AUP. Violating the terms of the AUP would be a student code of conduct violation and would be dealt with on the campus with a campus administrator.

Why can't my little brother bring his laptop to school? He is in the 4th grade.
Answer: Currently, we are limiting this privilege to 5th-12th students and staff.

Am I able to connect my laptop to an open network port and gain access to the internet?

Answer: No. CISD is only providing access to personal devices through the wireless network. *Under no circumstances can a personal device be plugged directly into the school network.*

Will there be a penalty to my grade if I do not have my own device?

Answer: No. Devices are never required and therefore, a grade cannot be taken.

Can The School Confiscate Or Search My Device?

Answer: Yes

- District staff may confiscate personal electronic devices when such devices are being used in violation of the AUP or school policies. Upon confiscation, district staff shall follow all district and school procedural directives and processes.

- District staff may search confiscated personal electronic devices and examine the content of students' personal electronic devices when there is reasonable suspicion of unauthorized or illegal use of the devices and may turn the devices over to the proper authorities for further investigation when warranted. When determining if a search is appropriate, district staff shall ensure the following conditions are met before conducting the search:

    a. The search is reasonable at its inception. That is, when the context is such that it is clear that the student or students are clearly misusing the device and that the search of content would turn up evidence of the violation.
    b. The scope of the search of the content is reasonably related to the objective of the search and appropriate in light of the age and sex of the student and the nature of the suspected violation.

At the conclusion of the investigation the device will be returned to the student or guardian.

STAFF

Do I, as the teacher, have the choice when students can use their technology devices?

Answer: Students may use technology at the discretion of the teachers as the lesson warrants the use.

Some of my students cannot access the network on their laptops or phones. I don't have time in a class period to help them with this. Should I put in a help request or call the help desk?

Answer: No. Students who cannot access the CISD PirateNet wireless network, or who may have technical issues with their technology tool, need to take care of this issue out of the classroom by working with their user's manual that came with the device. These are not CISD devices, and the district is not allocating resources at this time to troubleshoot issues. You are welcome to help if you choose, but it is not a staff member's responsibility to ensure that student owned technology is functioning properly.

I have students on my campus who are accessing the Internet using their provider's data plan (AT&T, Sprint, Verizon etc.) on their smart phones or laptops, hence bypassing the filter. Is this a violation of the student AUP?

Answer: This is not an AUP violation because the student is not bypassing the filter on the CISD network, but instead using a provider's data plan. Students who access inappropriate content at school are in violation of school rules regardless of how they obtain the content.

I have my own laptop and a smart phone. I would like to utilize these tools at work. Does this new plan include campus staff?

Answer: Yes. Campus staff can also access the PirateNet wireless network. Campus printers will not be accessible with your own devices. When prompted, choose **PirateNet** from the list. Once you choose this network, you will be prompted to accept the terms of service.

One of my students was using his laptop/device to bully another student on campus. Should I call the central technology office concerning this problem?

Answer: No. Any disciplinary infractions that occur from using technology tools should be referred to a campus administrator. This would be a student code of conduct issue.

Will students have access to any common software packages via the PirateNet wireless network access?

Answer: High School students (7-12) with gaggle accounts will have access to a full range of productivity type tools. However, no CISD software packages will be made available over the wireless connection. This is due to license and technological limitations.

Should I call central office if one of my student's laptops is damaged or stolen?
Answer: No. Any theft issues should be handled as you normally would on your campus. CISD is not responsible for any damage or theft of student owned technology tools. It would be good to remind students to keep a record of the device's serial number just in case a theft occurs.

PARENTS

My son is bringing his iPad to school for instructional purposes. Will he have access to things he normally does with district equipment?

Answer: Your son will have access to any of the web based software high school campuses currently use (Databases, library search tools etc.). Software may run differently on different devices for varying reasons. You should consult your owner's manual for software limitations. (Ex., iPads cannot run software requiring Flash Player.)

As a parent, am I required to add additional software (virus protection, filter, tracking device, etc.) to my child's technology tool?

Answer: No. Currently we are not requiring any additional software for school use. Virus protection is always advised, but not required to participate. While on the PirateNet network, students will be monitored through the district's filter, so there is no need for additional filtering software.

I have read the terms of service and I do not wish to have my child accessing the Internet using her own laptop. I would like to allow her to use her computer for productivity, but not the Internet. Is this possible within this pilot plan?

Answer: Yes. Your daughter may choose not to accept the terms of use; however, the rules outlined in the *Acceptable Use Policy* still apply for technology use of any kind (Internet or other). Also, it is not the responsibility of campus staff to ensure she has not accessed the Web on her own technology device. Damage or theft is still the responsibility of the owner.

If my child's laptop is stolen or damaged, what recourse can I take?

Answer: The district is not responsible for any damage or theft of student owned equipment. Installing tracking software or apps can help locate the equipment if it is stolen, and keeping track of the device's serial number, model and type will be helpful as well. Theft or vandalism of any kind should be reported immediately to the principal so he/she can take the appropriate steps.

What are the campus/classroom rules for using student owned devices including phones?
Answer: Teachers make the final decision for any tools used in the classroom; student owned equipment would be no different. It will be up to the individual teachers to communicate their expectations to parents and students. Please refer to the student handbook for further details.

Will my child have access to communication tools like email or message boards while on the PirateNet network?

Answer: **Yes.** Students do have access to their email accounts.

Collinsville ISD Internet Safety Plan

1. The district is providing Internet access to its employees, staff, and students. The district's Internet system has a limited educational purpose. 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.

2. Student use of the district's Internet system will be governed by this document, the district's Acceptable Use Policy (AUP), related district and school regulations, and the student disciplinary code. Staff use will be governed by this document, related district policies and regulations, district employment policy.

Internet system

1. Users should have limited or no privacy expectations regarding the contents of their personal files and records of their online activity while on the district system.

3. The district may restrict access to materials for valid educational reasons.

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

a. The district promotes the effective, educational use of the Internet in school through professional development and the establishment of a district web site.

b. Student and staff users of the district Internet system have been informed regarding the safe, ethical, legal, and responsible use of the Internet and of the district's Internet system and their responsibilities under this plan.

c. Student use and activities will be structured in a manner that is appropriate to the age and skills of students.

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

i. 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 a teacher or by staff 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.

ii. 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, CISD does not rely on filters as a sole protection measure.

iii. 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.

iv. 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.

iiv. 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.

iiiv. The district has developed procedures to monitor student use of the Internet.

ix. The AUP includes provisions that address the following safe and responsible use issues:

1. Access to inappropriate material.

2. Privacy and communication safety standards for self and others

3. 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.

4. Inappropriate language.

5. Plagiarism and copyright infringement.

6. Actions or use that may disrupt or jeopardize the security or effective performance of the district's network or the Internet.

7. Safety and security when using direct electronic communication

8. 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.

9. The district will develop regulations addressing the disclosure of student information, posting student-created material, and posting pictures of students on the district web site and district social media sites. (see web publishing procedure).

10. Each school year, parents/guardians must sign an agreement to allow their child to access the Internet.

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

10. The district has developed district web site guidelines to promote the effective educational use of the Internet, protect the privacy rights and other rights of students and staff, placement of material, and present an image that will reflect well on the district, schools, staff, and students.

12. The administrative responsibilities of the district administrative staff related to the district Internet system are as follows:

a. The superintendent, or his/her designee, will serve as the coordinator to oversee the district Internet system. The superintendent is 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.

b. The building administrator, 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.

c. 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 of Electronic Communications

Acceptable Use Policy Required Signatures:

Student

I understand and will abide by the provisions and conditions of this contract. I understand that any violations of the above provisions may result in disciplinary action, the revoking of my user account, and appropriate legal action. I also agree to report any misuse of the information system to the District WAN/LAN/system administrator. Misuse can come in many forms, but can be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, bullying, and other issues described above. I also understand the school guidelines for publishing on the school website and online. All the rules of conduct described in the District Code of Conduct and the High School Student Handbook apply when I am on the school network.

I also understand and agree to abide by both the web safety and district web publishing guidelines as published in the current student code of conduct. I understand that student photos, projects, videos, artwork and other content may be published to the school website, and district or teacher professional social media pages.

Student Name (please print): _____

Student Signature _____ Date _____/__/___

Parent or Guardian

Students under the age of 18 must also have the signature of a parent or guardian who has read this contract. As the parent or guardian of this student, I have read this contract and understand that it is designed for educational purposes. I understand that it is impossible for Collinsville Independent School District to restrict access to all controversial materials, and I will not hold the District Responsible for materials acquired on the network. I also agree to report any misuse of the information system to the District WAN/LAN/system administrator. Misuse can come in many forms, but can be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, bullying, inappropriate language, and other issues described above. I also understand the school guidelines for publishing on the school website and online. I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give my permission to issue an computer account for my child and certify that the information contained on this form is correct. I also understand and agree that my student will abide by both the web safety and district web publishing guidelines as published in the current student code of conduct. I understand that student photos, projects, videos, artwork and other content may be published to the school website, and district or teacher professional social media pages.

Parent or Guardian Name (please print): _____

Signature _____ Date _____/__/___