Central Community High School District #71
Acceptable Use Policy

Central Community School District #71 is pleased to have technology and networks available to access the Internet, publish web pages and communicate using e-mail. Hardware is in place for students to access educational resources from anywhere in the world. Students may use computers to enhance lessons, research topics, build academic skills and extend learning beyond the classroom.

Along with access to the Internet also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The District Acceptable Use Policy restricts access to material that is inappropriate in the school environment and the District has taken available precautions to restrict access to controversial materials. However, on a global network, it is impossible for filtering software to block every controversial and inappropriate site.

The Board of Education recognizes that although the Internet and on-line services afford access to legitimate sources of information for academic and educational purposes, they also enable access to materials which may be illegal, obscene or indecent. The use of elements of the District Technology System including the Internet shall be consistent with the District's educational mission and the curriculum adopted by the Board.

The "System" shall include all computer hardware and software owned or operated by the District, the District electronic mail, the District web site, and the District online services. "Use" of the System shall include use of or obtaining access to the System from any electronic device whether owned or operated by the District.

PURPOSE OF TECHNOLOGY

District technology, computers, and access to the Internet are designed for educational purposes only. The term "educational purpose" includes use of the network (hardware/software/connections, etc.) and access to the Internet for classroom activities, research, communications, career awareness, and professional development. Use of these educational tools is a privilege, not a right, and inappropriate use will result in the suspension or revocation of those privileges.

The District reserves and retains the right to regulate the content of and links to the District Technology System. The District also has the right to and does monitor use of its Technology System. Except as provided by federal and state statutes protecting the confidentiality of students' education records, no user of the District Technology System has an expectation of privacy in connection with such use.

Student use of technology, Internet, web publications and e-mail will be governed by the policies found in this document, related District regulations, and student disciplinary code. Violation of the acceptable use guidelines shall be subject to consequences including but not limited to discipline, loss of System use privileges, and referral to law enforcement authorities or other legal action in appropriate cases.

The District has the right to access, review, copy, delete, or disclose, as allowed by law, any message sent, received, or stored on the District's electronic mail system. The District has the right to and does monitor use of the System by students, including students' access to the Internet, as part of System maintenance to determine whether the use is consistent with federal and state laws and District policies and guidelines. All users should be aware that their personal computer files or System use may be subject to public disclosure under the *Illinois Freedom of Information Act*.

Use of the technology, Internet, web publications and e-mail constitutes consent to abide by the policies contained in this document.

With respect to any district-owned devices with Internet access on school grounds, the District will use technology protection measures to make a reasonable effort to (A) protect minors against access through such devices to visual depictions which are obscene, constitute child pornography, or are otherwise harmful to minors, and (B) protect all users against access through such devices to visual depictions that are obscene or constitute child pornography and (C) address the safety and security of all users using email, chat rooms, or other direct communications.

TECHNOLOGY AND COMPUTER USE

All students shall assume the following responsibilities while using District technology and computers.

- Students will treat equipment with care and report any abuse or misuse to the appropriate personnel.
- Students will report any malfunction or problem as soon as they become aware of it to appropriate personnel.
- Students shall not attach any devices to the District Network without district consent and approval. This includes devices that connect wirelessly to the District Network.
- Students will not vandalize or otherwise **intentionally** damage any District technology hardware or software. If they do, they or their parents/legal guardians will be responsible to pay all repair and/or replacement costs. Vandalism is defined as any malicious attempt to harm or destroy data of another person, computer software, the network, computer hardware, computer wiring, or computer configuration.
- Students will not damage, destroy, or copy another person's data. If they do they will be referred to the building principal. ***Incidents in which a student copies another student's data or does not cite work done by other people will be treated as cheating.***
- Students will not tamper with or attempt to gain access to computer data to which they have no security authorization. Doing so will result in the suspension or revocation of the user's privileges, disciplinary action, and/or appropriate legal action.
- Students will not load or copy unauthorized software onto District computers. All software used on District computers is to be properly licensed and registered with the publisher or manufacturer, and ***installed by District Technology personnel***.
- Students will not attempt to log-in to a computer or the District's network as a system administrator. Doing so will result in the revocation of the user's network privileges, disciplinary action, and/or appropriate legal action.
- Students identified as a security risk may be denied access to the District's technology and computers.

ACCESS

Students may be provided with either a classroom or individual account. All students are prohibited from sharing their log-in IDs or passwords with any other individual. Any attempt to log in as another user will result in discipline. ***Students will be granted access to the District's technology, networks and Internet unless the student's parent or legal guardian request in writing that their (child) ren should not be provided access.***

INTERNET USE

The District's access to the Internet, and its software, hardware, and data files, are owned and controlled by the School District. The District provides Internet access to all individuals as an educational tool. The District maintains the right to monitor Internet use and maintain user logs. All users shall assume the following responsibilities while using the Internet.

PROHIBITED RESOURCES

The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

1. Engage in activities which are not related to District educational purposes or which are contrary to the instructions from supervising District employees as to the System's use.
2. Access, retrieve, or view obscene, hateful, profane or indecent materials.
3. Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulation or District policy or rules. This includes, but is not limited to, improper use of copyrighted material; improper use of the System to commit fraud or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any student, District employee, or System user.
4. Transfer any software to or from the System without authorization from the System Administrator.
5. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.
6. Harass, threaten, intimidate, or demean an individual or group of individuals because of race, color, religion, sex, national origin, ancestry, age, order of protection status, marital status, physical or mental disability, military status, or sexual orientation.
7. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.
8. Disrupt or interfere with the System.
9. Gain unauthorized access to or vandalize the data or files of another user.
10. Gain unauthorized access to or vandalize the System or the technology system of any other individual or organization.

11. Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password or that of another user.
12. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of individual records.
13. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.
14. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.
15. Send mass electronic mail to multiple users without prior authorization by the appropriate District Administrator.
16. Conceal or misrepresent the user's identity while using the System.
17. Post material on the District's web site without the authorization of the appropriate District administrator.
18. Attempt to gain unauthorized access to the District network or use the District's network to access any other computer system. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".
19. Make deliberate attempts to disrupt computer performance or destroy data by any means including spreading computer viruses or hacking. These actions are illegal.
20. Use the District's networks to engage in any other illegal acts, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, etc.
21. Use data created outside the school and brought in on other media types without permission from the teacher and scanning the data for viruses.
22. Use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
23. Engage in personal attacks, including prejudicial or discriminatory attacks, or knowingly or recklessly post false or defamatory information about a person or organization.
24. Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending him/her messages, the student must stop.
25. Post personal contact information about themselves or other people. Personal contact information includes full names, address, telephone number, school address, work address, etc. Students will not post private information about another person.
26. Agree to meet with someone they have met online without their parent's approval and participation.
27. Repost a message that was sent to them privately without permission of the person who sent the message.
28. Plagiarize another person's work. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
29. Infringe on another person's rights of copyright. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request written permission from the copyright owner.
30. Post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
31. Conduct random Internet searches that are unrelated to the specific lesson for which the System is being used.
32. Accessing or attempting "proxy" based web sites.
33. Using the network while access privileges are suspended or revoked.
34. Using the network to perform any acts of cyber-bullying, cyber-harassment or cyber-stalking.

WEB PAGE PUBLISHING GUIDELINES

Any web site created by a student using the System must be part of a District-sponsored activity, or otherwise be authorized by the appropriate District administrator. All content, including links, of any web site must receive prior approval by an appropriate District administrator. All contents of a web site must conform to these Acceptable Use Guidelines. All students shall assume the following responsibilities while producing student web pages that are created and posted for outside viewing:

a. Students will be allowed to create "content" pages related to a specific class activity under the supervision of their teacher. Content pages must be related to meeting the educational objectives of the curriculum.
b. Students will not be allowed to publish "personal" web pages on the District's server.
c. Student web pages will be removed at the end of the school year unless special arrangements are made.

d. Student web pages must include a statement that identifies the page as a student created web page.

Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

E-MAIL USE

The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District may provide email to aid students as an education tool.

a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an email account is strictly prohibited.
b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
e. Use of the School District's email system constitutes consent to these regulations.

OFF CAMPUS COMPUTER USE

Using a home-based or off-campus computer such that the use results in material and/or substantial disruption to the school and/or a true threat will constitute grounds to investigate whether the use violates applicable law or school rules. Should such misuse be determined, the student may receive disciplinary consequences appropriate for the frequency and severity of the violation.

MOBILE DEVICE POLICY

The District may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; the District is entrusting the device to your care. Users should immediately report any loss, damage, or malfunction to a Technology Department employee. Users may be financially accountable for any damage resulting from the negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

SOCIAL MEDIA

The District may provide access to social networks, blogs, Internet forums and wikis for the purpose of educational needs. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube, Google+, and Flickr. Social media sites must be used only for educational and school related purposes, in connection with lessons and assignments to facilitate communication with teachers and other students. Access for students will be limited in nature and be fully supervised.

NON-SCHOOL-SPONSORED PUBLICATIONS/WEBSITES

Students are prohibited from accessing and/or distributing at school any pictures, written material, or electronic material, including material from the Internet or from a blog, that: 1) will cause substantial disruption of the proper and orderly operation and discipline of the school or school activities; 2) violates the rights of others, including but not limited to material that is libelous, invades the privacy of others, or infringes on a copyright; 3) is socially inappropriate or inappropriate due to maturity level of students, including but not limited to material that is obscene, pornographic, or pervasively lewd and vulgar, or contains indecent and vulgar language; or 4) is primarily intended for the immediate solicitation of funds. Nothing herein shall be interpreted to prevent the inclusion of material from outside sources or the citation to such sources as long as the material to be distributed or accessed is primarily prepared by students. *The distribution of non-school-sponsored written material must*

occur at a time and place and in a manner that will not cause disruption, be coercive, or result in the perception that the distribution or the material is endorsed by the school district.

VIOLATIONS OF COMPUTER AND/OR INTERNET USE

The failure of any student to follow the terms of the Central Community High School District No. 71's Technology and Acceptable Use Policy Agreement will result in loss or restricted computer use (including Internet access), disciplinary action and/or appropriate legal action. The Superintendent or designee and/or Building Principal will make all decisions regarding whether or not a user has violated the Technology and Internet Acceptable Use Policy and may deny, revoke, or suspend access at any time.

DUE PROCESS

The District will cooperate fully with local, state, or federal officials in any investigation concerning correlating to any illegal activities conducted through the District's network.

In the event there is an allegation that a user has violated the District Acceptable Use Policy, the person will be provided with a notice and opportunity to be heard in the manner set forth in the disciplinary code. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the user in gaining the self-discipline necessary to behave appropriately on an electronic network. In the event there is an allegation that a user has violated the District Acceptable Use Policy, the person will be provided with a notice and opportunity to be heard in the manner set forth in the disciplinary code. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the user in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the disciplinary code, the violation will be handled in accord with the applicable provision of the code. **Disciplinary actions and consequences will be handled with regard to Central Community High School District 71 regulations and applicable Board Policy.**

SEARCH AND SEIZURE

Students have a limited expectation of privacy with regard to the contents of their personal files, and online activity may be monitored while using the District's network.

Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Acceptable Use Policy. If this occurs the student disciplinary code, District regulations, and/or the law will be used to resolve this situation.

An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the student disciplinary code.

WARRANTY

The School District makes no warranties of any kind, whether expressed or implied, for the service it is providing nor is it responsible for any damages suffered by a user. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or the user's errors or omissions. Use of any information is at the users own risk. The School District specifically denies any responsibility for the accuracy or quality of information obtained through its services. The District is not responsible for any user's intentional or unintentional access of material on the Internet which may be obscene, indecent, or of an inappropriate nature.

INDEMNIFICATION

The user agrees to indemnify the School District for any losses, cost, or damages, including reasonable attorney fees, incurred by the School District relating to, or arising out of, any breach of the authorization.

TELEPHONE CHARGES

The School District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, equipment or line cost, and/or any online purchases.

Central Community High School District #71
Acceptable Use Policy

I understand and will voluntarily abide by the Central Community High School Acceptable Use Policy. I further understand that any violation of the Acceptable Use Policy may result in my user access privileges being revoked and school disciplinary action being taken. The signature(s) on this document indicate(s) that I/we have read the Central Community High School Acceptable Use Policy, understand its significance and voluntarily agree to comply fully with all of its terms and conditions.

Date ____/____/____ User Name _____
(Please print)

User Signature _____

As the parent or guardian of the student who has signed above, I have read the Central Community High School District 71 Acceptable Use Policy. I understand that electronic use is designed for educational purposes and each student will have access to electronic devices as described in the Acceptable Use Policy. However, I recognize it is possible that my student may procure material that is not consistent with the educational goals of the Central Community High School. I also understand that if my student does not have my permission to have Internet access and he is involved in an activity where the class is using the Internet he/she will be given an alternative assignment of equivalent value. With this understanding I will mark below my preference as to whether Central Community High School should provide Internet access for my student and certify that the information contained on this form is correct.

_____ Yes, I give permission for the user listed above to have Internet access.

_____ No, I do not give permission for the user listed above to have Internet access.

Date ____/____/____ Parent/Guardian: _____
(Please Print)

Parent/Guardian: _____
(Signature)

Address: _____

_____

Media Photo/Information Release

I hereby give Central Community High School District 71 the unqualified right and permission to reproduce, copyright, publish, circulate, or otherwise use photographic reproductions or likenesses of me and/or my name. The authorization and release covers the use of said material in any published form, and any medium of advertising, or publicity. I hereby certify I am an adult above the age of twenty-one in consenting to the release of the above-mentioned photographic reproductions.

** In the event the person is not an adult over the age of twenty-one, the signature listed below is that of the adult or guardian responsible for the child.

Name of person for photo release: _____

Parent/Guardian Signature: _____

Date of Release: _____

Release Authorization is Indefinite with no specific expiration

****

For Office Use Only

Student ID: _____ ***Graduation Year: _____***