

Electronic Communications System

Definitions

1. “Technology protection measure,” as defined by the Children’s Internet Protection Act (CIPA) means a specific technology that blocks or filters Internet access to visual depictions that are:
 - a. Obscene, as that term is defined in Section 1460 of Title 18, United States Code;
 - b. Child pornography, as that term is defined in Section 2256 of Title 18, United States Code; or
 - c. Harmful to minors.
2. “Harmful to minors” as defined by CIPA means any picture, image, graphic image file or other visual depiction that:
 - a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
 - b. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 - c. Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.
3. “Sexual act; sexual contact” as defined by CIPA have the meanings given such terms in Section 2246 of Title 18, United States Code.
4. “Minor” as defined by CIPA means an individual who has not attained the age of 17. For the purposes of Board policy and this administrative regulation, minor will include all students enrolled in district schools.
5. “Inappropriate matter” as defined by the district means material that is inconsistent with general public education purposes, the district’s mission and goals.¹

General District Responsibilities

The district will:

1. Designate staff as necessary to ensure coordination and maintenance of the district’s electronic communications system which includes all district computers, e-mail and Internet access;

¹As inappropriate matter is not defined in the CIPA or regulations, districts should define the scope of what it will regard as inappropriate matter. The language provided in #5. is intended as a guide only.

2. Provide staff training in the appropriate use of the district's system including copies of district policy and administrative regulations. Staff will provide similar training to authorized system users;
3. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district's system;
4. Use only properly licensed software, audio or video media purchased by the district or approved for use by the district. The district will comply with the requirements of law regarding the use, reproduction and distribution of copyrighted works and with applicable provisions of use or license agreements;
5. Install and use desktop and/or server virus detection and removal software;
6. Provide technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or with respect to the use of computers by minors, harmful to minors. A supervisor or other individual authorized by the building principal may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate;
7. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web;
8. Provide staff supervision to monitor the online activities of students to prevent unauthorized access, including "hacking" and other unlawful activities online, and ensure the safety and security of minors when authorized to use e-mail, chat rooms and other forms of direct electronic communication;
9. Determine which users and sites accessible as part of the district's system are most applicable to the curricular needs of the district and may restrict user access, accordingly;
10. Determine which users will be provided access to the district's e-mail system;
11. Program its computers to display a message reinforcing key elements of the district's Electronic Communications System policy and regulation when accessed for use;
12. Notify appropriate system users that:
 - a. The district retains ownership and control of its computers, hardware, software and data at all times. All communications and stored information transmitted, received or contained in the district's information system are the district's property and are to be used for authorized purposes only. Use of district equipment or software for unauthorized purposes is strictly prohibited. To maintain system integrity, monitor network etiquette and ensure that those authorized to use the district's system are in compliance with Board policy, administrative regulations and law, the school administrators may routinely review user files and communications;

- b. Files and other information, including e-mail, sent or received, generated or stored on district servers are not private and may be subject to monitoring. By using the district's system, individuals consent to have that use monitored by authorized district personnel. The district reserves the right to access and disclose, as appropriate, all information and data contained on district computers and district-owned e-mail system;
 - c. The district may establish a retention schedule for the removal of e-mail;
 - d. E-mail sent or received by a Board member or employee in connection with the transaction of public business may be a public record and subject to state archivist rules for retention and destruction;
 - e. Information and data entered or stored on the district's computers and e-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the district. "Deleted" or "purged" data from district computers or e-mail system may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the district;
 - f. The district may set quotas for system disk usage. The district may allow system users to increase their quota by submitting a written request to the supervising teacher or system coordinator stating the need for the increase;
 - g. Passwords used on the district's system are the property of the district and must be provided to their supervisor or designated district personnel, as appropriate. Passwords that have not been provided to the district are prohibited;
 - h. Transmission of any materials regarding political campaigns is prohibited.
13. Ensure all student, staff and nonschool system users complete and sign an agreement to abide by the district's electronic communications policy and administrative regulations. All such agreements will be maintained on file in the school office;
14. Notify users of known copyright infringing activities and deny access to or remove the material.

System Access

1. Access to the district's system is authorized to:
- Board members, district employees, students in grades K-12, with parent approval and when under the direct supervision of staff, and district volunteers, district contractors or other members of the public as authorized by the system coordinator or district administrators consistent with the district's policy governing use of district equipment and materials.
2. Students, staff, Board members, volunteers, district contractors and other members of the public may be permitted to use the district's system for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/guidelines/etiquette and other applicable provisions of this administrative regulation. Personal use of district-owned computers including Internet and e-mail access by employees is prohibited during the employee's work hours. Additionally, Board member and employee use of district-owned computers may be permitted only when such use does not violate the provisions of ORS 244.040 and use is under the same terms and conditions that access is provided to the general public under the district's policy governing use of district equipment and materials.

General Use Prohibitions/Guidelines/Etiquette

Operation of the district's system relies upon the proper conduct and appropriate use of system users. Students, staff and others granted system access are responsible for adhering to the following prohibitions and guidelines which require legal, ethical and efficient utilization of the district's system.

1. Prohibitions

The following conduct is strictly prohibited:

- a. Attempts to use the district's system for:
 - (1) Unauthorized solicitation of funds;
 - (2) Distribution of chain letters;
 - (3) Unauthorized sale or purchase of merchandise and services;
 - (4) Collection of signatures;
 - (5) Membership drives;
 - (6) Transmission of any materials regarding political campaigns.
- b. Attempts to upload, download, use, reproduce or distribute information, data, software, or file share music, videos or other materials on the district's system in violation of copyright law or applicable provisions of use or license agreements;;
- c. Attempts to degrade, disrupt or vandalize the district's equipment, software, materials or data or those of any other user of the district's system or any of the agencies or other networks connected to the district's system;
- d. Attempts to evade, change or exceed resource quotas or disk usage quotas;
- e. Attempts to send, intentionally access or download any text file or picture or engage in any communication that includes material which may be interpreted as:
 - (1) Harmful to minors;
 - (2) Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district;
 - (3) A product or service not permitted to minors by law;
 - (4) Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others;
 - (5) A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
 - (6) Defamatory, libelous, reckless or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense or otherwise violates any law, rule, regulation, Board policy and/or administrative regulation.
- f. Attempts to gain unauthorized access to any service via the district's system which has a cost involved or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs;
- g. Attempts to post or publish personal student contact information unless authorized by the system coordinator or teacher and consistent with applicable Board policy pertaining to student

- directory information and personally identifiable information. Personal contact information includes photograph, age, home, school, work or e-mail addresses or phone numbers or other unauthorized disclosure, use and dissemination of personal information regarding students;
- h. Attempts to arrange student meetings with anyone on the district's system, unless authorized by the system coordinator or teacher and with prior parent approval;
 - i. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization;
 - j. Attempts to use another individual's account name or password, failure to provide the district with individual passwords or to access restricted information, resources or networks to which the user has not been given access.

2. Guidelines/Etiquette

System users will:

- a. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and administrative regulations;
- b. Respect other people's time and cyberspace. Use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher or system coordinator. Avoid downloading excessively large files. Remain on the system long enough to get needed information then exit the system. Act as though every byte sent costs somebody time and money, because it does;
- c. Take pride in communications. Check spelling and grammar;
- d. Respect the privacy of others. Do not read the mail or files of others without their permission;
- e. Cite all quotes, references and sources;
- f. Adhere to guidelines for managing and composing effective e-mail messages:
 - (1) One subject per message - avoid covering various issues in a single e-mail message;
 - (2) Use a descriptive heading;
 - (3) Be concise - keep message short and to the point;
 - (4) Write short sentences;
 - (5) Use bulleted lists to break up complicated text;
 - (6) Conclude message with actions required and target dates;
 - (7) Remove e-mail in accordance with established guidelines;
 - (8) Remember, there is no expected right to privacy when using e-mail. Others may read or access mail;
 - (9) Always sign messages;
 - (10) Always acknowledge receipt of a document or file.
- g. Protect password confidentiality. Passwords are the property of the district and are not to be shared with others. Using another user's account or password or allowing such access by another may be permitted with supervising teacher or system coordinator approval only. No system user may use a password on the district's computers, e-mail system or Internet access which is unknown to the district;
- h. Communicate only with such users and/or sites as may be authorized by the district;
- i. Be forgiving of the mistakes of others and share your knowledge. Practice good mentoring techniques;

- j. Report violations of the district's policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator, as appropriate.

Complaints

Complaints regarding use of the district's Electronic Communications System may be made to the teacher, principal, employee's supervisor or system coordinator. The district's established complaint procedure will be used for complaints concerning violations of the district's Electronic Communications System policy and/or administrative regulation. See Board policy KL and accompanying administrative regulation.

Violations/Consequences

1. Students
 - a. Students who violate general system user prohibitions shall be subject to discipline up to and including expulsion and/or revocation of district system access up to and including permanent loss of privileges.
 - b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
 - c. Disciplinary action may be appealed by parents, students and/or a representative in accordance with established district procedures.
2. Staff
 - a. Staff who violate general system user prohibitions shall be subject to discipline up to and including dismissal in accordance with Board policy, collective bargaining agreements and applicable provisions of law.
 - b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
 - c. Violations of applicable Teacher Standards and Practices Commission (TSPC), Standards for Competent and Ethical Performance of Oregon Educators will be reported to TSPC as provided by OAR 584-020-0041.
 - d. Violations of ORS 244.040 will be reported to GSPC.
3. Others
 - a. Other guest users who violate general system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.
 - b. Violations of law will be reported to law enforcement officials or other agencies, as appropriate, and may result in criminal or civil sanctions.

Telephone/Membership/Other Charges

1. The district assumes no responsibility or liability for any membership or phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment or line costs incurred by any home usage of the district's system.

2. Any disputes or problems regarding phone services for home users of the district's system are strictly between the system user and his/her local phone company and/or long distance service provider.

Information Content/Third Party Supplied Information

1. System users and parents of student system users are advised that use of the district's system may provide access to materials that may be considered objectionable and inconsistent with the district's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the district's system accordingly.
2. Opinions, advice, services and all other information expressed by system users, information providers, service providers or other third-party individuals are those of the providers and not the district.
3. System users may, with supervising teacher or system coordinator approval, order services or merchandise from other individuals and agencies that may be accessed through the district's system. These individuals and agencies are not affiliated with the district. All matters concerning merchandise and services ordered including, but not limited to, purchase terms, payment terms, warranties, guarantees and delivery are solely between the seller and the system user. The district makes no warranties or representation whatsoever with regard to any goods or services provided by the seller. district staff and administration shall not be a party to any such transaction or be liable for any costs or damages arising out of, either directly or indirectly, the actions or inactions of sellers.
4. 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. The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express 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.

Sample Parent Letter

Dear Parents:

Your student has [requested] [been selected] to participate in the district's electronic communications program and needs your permission to do so. Your student will be able to communicate with other schools, colleges, organizations and individuals around the world through the Internet and other electronic information systems/networks.

The Internet is a system which links networks creating a large and diverse communications network. Internet access allows your student the opportunity to reach out to many other people to share information, learn concepts and research subjects by the sending and receiving of messages using a computer, modem and phone lines.

With this educational opportunity also comes responsibility. It is important that you and your student read the enclosed district policy, administrative regulation and agreement form and discuss these requirements together. Inappropriate system use will result in discipline up to and including expulsion from school, suspension or revocation of your student's access to the district's system and/or referral to law enforcement officials.

Although the district is committed to practices that ensure the safety and welfare of system users, including the use of technology protection measures such as Internet filtering, please be aware that there may still be material or communications on the Internet that district staff, parents and students may find objectionable. While the district neither encourages nor condones access to such material, it is not possible for us to eliminate that access completely.

Attached to this letter are the following important documents:

1. An agreement for your student to read and sign stating his/her agreement to follow the district's Electronic Communications System policy and administrative regulation. This agreement requires your signature. It must be signed and renewed each year and will be kept on file at the school;
2. The district's Electronic Communications System policy and administrative regulation.

Please review these materials carefully with your student and return the attached agreement form to the [school office] indicating your permission or denial of permission for your student to participate in the district's electronic communications system.

Sincerely,

[System Coordinator/Administrator]

School Computer and Internet Use

Computers are available for students to use at school for school-related purposes. A signed Acceptable Use Agreement is REQUIRED of all students using the Internet while at school. Klamath Falls City Schools incorporates filtering software on all computers. However, no filtering software is perfect and responsibility also rests with the student to use the Internet appropriately.

Students who use the Internet for non-educational purposes will have their Internet privileges revoked for a minimum of one week. Students who attempt any hacking, virus planting or vandalism on school computers or networks will face severe disciplinary action that may include suspension or expulsion.

To read the complete Klamath Falls City Schools Acceptable Use Agreement, turn to pages 10 of this policy.

		First Occurrence		Second Occurrence	
Category	Offense	Access	Minimum Time	Access	Minimum Time
A	Student records	White list	2 weeks	No internet	4 weeks
	Non-approved activity	White list	2 weeks	No internet	4 weeks
	Bypass	White list	2 weeks	No internet	4 weeks
	Browser	White list	2 weeks	No internet	4 weeks
	Personal profiles	White list	2 weeks	No internet	4 weeks
	Porn (soft)	White list	2 weeks	No internet	4 weeks
	Downloads	White list	2 weeks	No internet	4 weeks
	Email	White list	2 weeks	No internet	4 weeks
	Block monitoring	White list	2 weeks	No internet	4 weeks
B	Sharing passwords	White list	4 weeks	No internet	9 weeks
C	Restricted CPU	Acct. Disabled	2 weeks	Acct. Disabled	9 weeks
D	Secure info	Acct. Disabled	18 weeks	Suspension/ expulsion	3 days
E	Porn (hard)	No internet	18 weeks	No internet	1 year
F	Vandalism, theft	Suspension/ expulsion	3 days + restitution	Expulsion	
	Hacking, interference	Suspension/ expulsion	3 days + restitution	Expulsion	

Multiple offenses receive the most severe punishment.

Second offense at a higher category receives that first offense penalty.

Second offense at a lower category receives that second offense penalty.

After the second offense, suspension or expulsion may result.

Computer use is a privilege, NOT A RIGHT!
Internet use is monitored and a permanent record is kept.

Klamath Falls City Schools Acceptable Use Agreement - Student
Please read this document carefully before signing.

Internet access is available to students and staff in the Klamath Falls City Schools. Our goal in providing this service is to promote educational excellence in schools by facilitating resource sharing, innovation, and communication.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Klamath Falls City Schools has taken precautions to restrict access to controversial materials. However, absolute restrictions are not possible due to the nature of the Internet. Klamath Falls City Schools believes that the advantages of Internet use outweigh the disadvantages.

Smooth operation of the network relies upon the proper conduct of the end users, who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical and legal utilization of the network resources. If a Klamath Falls City Schools user violates any of these provisions, his or her account may be restricted or terminated and future access could possibly be denied. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) this document.

Internet - Terms and Conditions

1. Acceptable Use – The use of your account must be in support of education and research and consistent with the educational objectives of the Klamath Falls City Schools. Use of other organization’s network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities, product advertisement, or political lobbying is generally not acceptable.
2. Privileges – The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as deemed necessary. The administration, faculty, and staff of Klamath Falls City Schools may request the system administrator to deny, revoke, or suspend specific user accounts.
3. Network Etiquette – You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:
 - a. Be polite. Do not get abusive in your messages to others.
 - b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
 - c. Do not reveal your personal address or phone numbers of students or colleagues.
 - d. Do not use the network in such a way that you would disrupt the use of the network by other users.
4. Klamath Falls City Schools makes no warranties of any kind, whether expressed or implied, for the service it is providing. Klamath Falls City Schools will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service

interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. Klamath Falls City Schools specifically denies any responsibility for the accuracy or quality of information obtained through its services. KFCS also assumes no financial responsibility.

5. Security – Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a system administrator or your District Internet Coordinator. Do not demonstrate the problem to other users. Do not use another individual’s account. You are responsible for any activity on your account. Students are not permitted to use computers logged in with staff accounts. Attempts to logon to the network as a system administrator will result in cancellation of user privileges. Attempting to acquire other user’s passwords is strictly prohibited. Any user identified as a security risk or having a history of violating our or other computer systems may be denied access to the network.
6. Vandalism - Vandalism is defined as any malicious attempt to harm or destroy the hardware, peripherals, server, or any other equipment associated with the network.
7. Hacking - Hacking is defined as any malicious attempt to harm or destroy data of another user, Internet, or attempting to gain unauthorized access to any network resources. This includes, but not limited to, the uploading or creation of computer viruses.

Internet Use Agreement Signature Section

I understand and will abide by the above Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.

User Name (please print): _____

User Signature: _____ Date: _____

PARENT OR GUARDIAN (Required if student is under the age of 18) As the parent or guardian of this student, I have read the Acceptable Use Agreement. I hereby give permission for my child to use the Internet at school.

Parent or Guardian’s Name (please print): _____

Signature: _____ Date: _____

SPONSORING TEACHER (Must be signed if the applicant is a student in grades K-6)

I have read the Internet Use Agreement and agree to promote this agreement, acceptable use of the network and proper network etiquette with the student. However, because the student may use the network for individual work or in the context of another class, I cannot be held responsible for the student use of the network.

Teacher’s Name (please print): _____

Signature: _____ Date: _____

Klamath Falls City Schools Acceptable Use Agreement - Staff
Please read this document carefully before signing.

Internet access is available to students and staff in the Klamath Falls City Schools. Our goal in providing this service is to promote educational excellence in schools by facilitating resource sharing, innovation, and communication.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Klamath Falls City Schools has taken precautions to restrict access to controversial materials. However, absolute restrictions are not possible due to the nature of the Internet. Klamath Falls City Schools believes that the advantages of Internet use outweigh the disadvantages.

Smooth operation of the network relies upon the proper conduct of the end users, who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical and legal utilization of the network resources. If a Klamath Falls City Schools user violates any of these provisions, his or her account may be restricted or terminated and future access could possibly be denied. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) this document.

Internet - Terms and Conditions

1. Acceptable Use – The use of your account must be in support of education and research and consistent with the educational objectives of the Klamath Falls City Schools. Use of other organization’s network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities, product advertisement, or political lobbying is generally not acceptable.
2. Privileges – The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as deemed necessary. The administration, faculty, and staff of Klamath Falls City Schools may request the system administrator to deny, revoke, or suspend specific user accounts.
3. Network Etiquette – You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:
 - a. Be polite. Do not get abusive in your messages to others.
 - b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
 - c. Do not reveal your personal address or phone numbers of students or colleagues.
 - d. Do not use the network in such a way that you would disrupt the use of the network by other users.
4. Klamath Falls City Schools makes no warranties of any kind, whether expressed or implied, for the service it is providing. Klamath Falls City Schools will not be responsible for any damages you

suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. Klamath Falls City Schools specifically denies any responsibility for the accuracy or quality of information obtained through its services. KFCS also assumes no financial responsibility.

5. Security – Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a system administrator or your District Internet Coordinator. Do not demonstrate the problem to other users. Do not use another individual’s account. You are responsible for any activity on your account. Students are not permitted to use computers logged in with staff accounts. Attempts to logon to the network as a system administrator will result in cancellation of user privileges. Attempting to acquire other user’s passwords is strictly prohibited. Any user identified as a security risk or having a history of violating our or other computer systems may be denied access to the network.
6. Vandalism – Vandalism is defined as any malicious attempt to harm or destroy the hardware, peripherals, server, or any other equipment associated with the network.
7. Hacking – Hacking is defined as any malicious attempt to harm or destroy data of another user, Internet, or attempting to gain unauthorized access to any network resources. This includes, but not limited to, the uploading or creation of computer viruses.
8. Electronic Mail – Email is not guaranteed to be private. System administrators may have access email. Email sent over the Internet is subject to interception by outside sources. Messages relating to or in support of illegal activities may be reported to the authorities. All communications accessible via the KFCS network should be assumed to be the property of KFCS.

Internet Use Agreement signature section

I understand and will abide by the above Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action or legal action may be taken.

User Name (print) _____

User Signature: _____ Date: _____