Forest City Regional School District

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY

ADOPTED: August 8, 2005

REVISED: September 16, 2013

	815. ACCEPTABLE USE OF TECHNOLOGY
1. Purpose	The Board supports use of the computers, Internet and other network resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. For instructional purposes, the use of network facilities will be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.
2. Definitions 18 U.S.C Sec. 2256	The term child pornography is defined under both federal and state law. Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 2. Such visual depiction' is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. Child pornography - under state law, is any book, magazine, pamphlet, slide,

18 Pa. C.S.A. Sec. 6312	photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act. The term harmful to minors is defined under both federal and state law. Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:
20 U.S.C. Sec 6777 47 U.S.C. Sec. 254	1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion; 2. 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 lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors; 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.
18 Pa. C.S.A. Sec. 5903	Obscene - any material or performance, if: 1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest; 2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and 3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

47 U.S.C. Sec. 254	Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.
3. Authority	The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district will not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The district will not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources. **Use of any Internet Source Provider that is not provided through the school district's network is strictly prohibited *unless approved by administration*, this includes cellular internet enabled phones, cellular air cards, and personal cellular "hot spots." Use of any rogue network, will be denied access upon detection.**
Pol. 218, 233, 317	The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users will have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district will cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources. The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.
47 U.S.C Sec. 254	The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: { } Defamatory. { } Lewd, vulgar, or profane. { } Threatening.

Pol. 103, 103.1, 104, 248, 348	{ } Harassing or discriminatory.
Pol. 249	{ } Bullying.
Pol. 218.2	{ } Terroristic.
	{ }_____ (specify others).
24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure will be enforced during use of computers with Internet access.
24 P.S. Sec. 4604	Upon request by students or staff, the Superintendent or designee will expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.
24 P.S. Sec. 4610 20 U.S.C. Sec. 6777	Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.
4. Delegation of Responsibility	The district will make every effort to ensure that this resource is used responsibly by students and staff.
24 P.S. Sec. 4604	The district will inform staff, students, parents/guardians, and other users about this policy through employee and student handbooks, posting on the district web site, and by other appropriate methods. A copy of this policy will be provided to parents/guardians, upon written request. Users of district networks or district-owned equipment will, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use { } and tracking systems to track and recover lost or stolen equipment. Student user agreements will also be signed by a parent/guardian.

	Student user agreements will also be signed by a parent/guardian. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet. Building administrators will make initial determinations of whether inappropriate use has occurred.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Superintendent or designee will be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures will include but not be limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254 SC 1303.1-A Pol. 249	The Superintendent or designee will develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking web sites and in chat rooms. 2. Cyberbullying awareness and response.
5. Guidelines	**3. The district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms; and cyberbullying awareness and response. The district will provide this instruction through the iSafe curriculum or other similar programs** Network accounts will be used only by the authorized owner of the account for its approved purpose. Network users will respect the privacy of other users on the system.

47 U.S.C.
Sec. 254
47 CFR
Sec. 54.520

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site will report such immediately to a teacher or administrator. Network users will not reveal personal information to other users on the network, including chat rooms, e-mail, social networking web sites, etc.

Internet safety measures will effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and WorId Wide Web.

2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.

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

5. Restriction of minors' access to materials harmful to them.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.

2. Commercial or for-profit purposes.

SC 1303.1-A
Pol. 249

3. Nonwork or nonschool related work.

4. Product advertisement or political lobbying.

5. Bullying/Cyberbullying.

6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.

Pol. 237

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

Pol. 814	8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs. 9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy. 10. Inappropriate language or profanity. 11. Transmission of material likely to be offensive or objectionable to recipients. 12. Intentional obtaining or modifying offiles, passwords, and data belonging to other users. 13. Impersonation of another user, anonymity, and pseudonyms. 14. Fraudulent copying, communications, or modification of materials in violation of copyright laws. 15. Loading or using of unauthorized games, programs, files, or other electronic media. 16. Disruption of the work of other users. 17. Destruction, modification, abuse or unauthorized access to network hardware, software and files. 18. Accessing the Internet, district computers or other network resources without authorization. 19. Disabling or bypassing the Internet blocking/filtering software without authorization. 20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization. <u>Security</u> System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines will be followed: 1. Employees and students will not reveal their passwords to another individual. 2. Users are not to use a computer that has been logged in under another student's

17 U.S.C. Sec. 101 et seq Pol. 814	or employee's name. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. <u>Copyright</u> The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network will be subject to fair use guidelines and applicable laws and regulations. <u>Deep Packet Inspection</u> Through the use of a technology protective device, district traffic will be intercepting all digital communication prior to sending the digital communication to the Internet. The district will have the capability to decrypt and monitor all traffic including email, online banking, social networking, and any other web site that uses SSL or similar encryption protocols. <u>Electronic Mail and Digital Communication</u> The use of district electronic mail and digital communication is to communicate for school district business. Every electronic mail or digital communication sent will abide by the Family Educational Rights and Privacy Act and Health Insurance Portability and Accountability Act. Student's names should never be fully mentioned in any electronic mail or digital communication, except for their initials. No Health information is to be discussed in electronic mail or digital communication. Electronic Mail will be archived minimally for seven years. <u>Personal Equipment Policy</u> The use of personal equipment, to access electronic mail and digital communication through personal tablets, smart phones, and other similar devices that bind to our servers/network, will be allowed for users, approved by administration. With binding to our servers/network, the district has the right to either remotely remove district accounts from the devices or remotely wipe to factory settings when computer equipment or accounts are compromised.
24. P.S. Sec. 4604	<u>District Web Site</u> The District {X} will

	{ } may establish and maintain a web site and will develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district web site will comply with this and other applicable district policies.
Pol. 218, 233, 317	Users will not copy or download information from the district web site and disseminate such information on unauthorized web pages without authorization from the building principal.
	Consequences For Inappropriate Use The network user will be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Vandalism will result in loss of access privileges, disciplinary action, and/or legal proceedings. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses. Failure to comply with this policy or inappropriate use of the Internet, district network or computers will result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.
	References: School Code - 24 P.S. Sec. 1303.l-A PA Crimes Code - 18 Pa. C.S.A. Sec. 5903, 6312 Child Internet Protection Act - 24 P.S. Sec. 4601 et seq. U.S. Copyright Law -17 U.S.C. Sec. 101 et seq. Sexual Exploitation and Other Abuse of Children -18 U.S.C. Sec. 2256

	Enhancing Education Through Technology Act - 20 U.S.C. Sec. 6777 Internet Safety, Children's Internet Protection Act - 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations - 47 CFR Sec. 54.520 Board Policy- l03, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814

FOREST CITY REGIONAL SCHOOL DISTRICT
ACCEPTABLE USE POLICY AGREEMENT FOR COMPUTING AND INTERNET ACCESS

READ CAREFULLY, COMPLETE, AND RETURN TO MAIN BUILDING OFFICE AS SOON AS POSSIBLE. PARENT(S)/GUARDIAN(S) SHOULD SIGN EITHER COMPUTERS/INTERNET OR COMPUTERS ONLY.

User
(For Students or District Employees)

I will abide by the above Terms and Conditions of the Forest City Regional School District Acceptable Use Policy 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, and school disciplinary action and/or other appropriate legal action may be taken.

User Name (please print) _____

User Signature: _____ Date: _____/_____/_____

Parent or Guardian
(For Parents or Guardians Only)

As the parent or guardian of this student, I have read the Terms and Conditions of the Forest City Regional School District Acceptable Use Policy agreement. I understand that this access is designed for educational purposes and Forest City Regional School District has taken numerous precautions to eliminate controversial material. I also recognize it is impossible for Forest City Regional School District to restrict access to all controversial materials. I will not hold them responsible for materials acquired on the network. I hereby give permission to issue an account for my child to use computers and the Internet and certify that the information contained on this form is correct.

Parent or Guardian Name (please print) _____

Signature: _____ Date: _____/_____/_____