SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (ACCEPTABLE USE POLICY)

The Board of Education will provide access to various computerized information resources through the District's computer system ("DCS" hereafter) consisting of software, hardware, computer networks and electronic communications systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may include the opportunity for some students to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use off school premises, shall be subject to this policy and accompanying regulations. Further, all such use must be in support of education and/or research and consistent with the goals and purposes of the School District.

Access to Inappropriate Content/Material and Use of Personal Technology or Electronic Devices

This policy is intended to establish general guidelines for the acceptable student use of the DCS and also to give students and parents/guardians notice that student use of the DCS will provide student access to external computer networks not controlled by the School District. The District cannot screen or review all of the available content or materials on these external computer networks. Thus some of the available content or materials on these external networks may be deemed unsuitable for student use or access by parents/guardians.

Despite the existence of District policy, regulations and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access such content or material from their home, other locations off school premises and/or with a student's own personal technology or electronic device on school grounds or at school events. Parents and guardians must be willing to establish boundaries and standards for the appropriate and acceptable use of technology and communicate these boundaries and standards to their children. The appropriate/acceptable use standards outlined in this policy apply to student use of technology via the DCS or any other electronic media or communications, including by means of a student's own personal technology or electronic device on school grounds or at school events.

Standards of Acceptable Use

Generally, the same standards of acceptable student conduct which apply to any school activity shall apply to use of the DCS. This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate student conduct and use as well as proscribed behavior.

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (ACCEPTABLE USE POLICY) (Cont'd.)

District students shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and student rights of privacy created by federal and state law.

Students who engage in unacceptable use may lose access to the DCS in accordance with applicable due process procedures, and may be subject to further discipline under the District's school conduct and discipline policy and the District Code of Conduct. The District reserves the right to pursue legal action against a student who willfully, maliciously or unlawfully damages or destroys property of the District. Further, the District may bring suit in civil court against the parents/guardians of any student who willfully, maliciously or unlawfully damages or destroys District property pursuant to General Obligations Law Section 3-112.

Student data files and other electronic storage areas will be treated like school lockers. This means that such areas shall be considered to be School District property subject to control and inspection. The Computer Coordinator may access all such files and communications without prior notice to ensure system integrity and that users are complying with the requirements of this policy and accompanying regulations. Students should **NOT** expect that information stored on the DCS will be private.

Notification

The District's Acceptable Use Policy and Regulations will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and students' obligations when accessing the DCS.

Regulations will be established as necessary to implement the terms of this policy.

NOTE: Refer also to Policy #8271 -- Internet Safety/ Internet Content Filtering Policy
District Code of Conduct on School Property

Adoption Date: 1/6/16

SUBJECT: INTERNET/COMPUTER USE STANDARDS

Use Authorized by Alexander Central School District Policy

a) Students shall be authorized to use the Alexander Central School District Internet facilities and connections for study, research and communications related to their assigned course work and approved co-curricular activities.

b) Use of data encryption techniques is prohibited.

c) Teachers, other members of the instructional staff and administrators shall be authorized to use District Internet facilities and connections for instruction, professional development and training, and research and communications related to curriculum and approved co-curricular activities. Instructional use of the Internet is governed by District policies, practices and procedures concerning the acquisition and use of textbooks, library books and non-print media.

d) Administrators, supervisors and support staff shall be authorized to use District Internet facilities and connections associated with their assigned areas of responsibility.

Unauthorized And Illegal Uses

Any use, whether onsite or offsite, of District Internet facilities and connections, not authorized by, nor conducted strictly in compliance with District policy, practices and procedures, and user agreements, is prohibited. Use of the Internet to commit a crime is prohibited. In addition, users are advised of the following specific unauthorized and illegal uses:

a) Copyright. Users are personally responsible for observing copyright laws in their use of the Internet. Users may face serious civil and/or criminal penalties for any violation of the copyrights of others. User must obtain the consent of the copyright owner before they copy, download, transmit, retransmit or alter copyrighted material, other than as permitted by the principle of fair use as defined in the copyright law.

b) Obscene materials. There are various State and Federal laws prohibiting the making and distributing of obscene materials. Use of District Internet facilities to make, transmit or receive obscene materials is prohibited and will result in disciplinary or legal action against the violator.

(Continued)

SUBJECT: INTERNET/COMPUTER USE STANDARDS (Cont'd)

c) Commercial activities. Users are prohibited from using the Internet/Electronic Mail to engage in the promotion or sale of any commercial or noncommercial products or services. Individual users are also responsible for refraining from acts that waste resources. These acts will include, but are not limited to, commercial or personal advertising, mass mailing for other than educational purposes, political fundraising, lobbying and other activities that detract from the educational mission of the District. These actions will result in denial of access.

d) Viruses and sabotage. No person may communicate any system virus through the Internet or engage in any activity intended to disrupt or damage hardware or software.

Internet Etiquette

Users of the Internet are expected to treat others with respect. This means:

a) Use only the same polite and respectful language to communicate on the Internet as would be appropriate in face-to-face communications in school. Accessing or disseminating information that is illegal, defamatory, abusive, racially offensive, and/or adult-oriented will be deemed a violation of this regulation which could result in disciplinary and/or legal action against the violator.

b) Respect your own privacy and the privacy of others by not revealing your or anyone else's personal address, telephone number or password without his/her authorization.

c) Treat the communications, information and databases you may gain access to through the Internet as private property. Use them only in ways for which you are sure that you have permission.

Security of System

a) The Internet is a voluntary network with no central administration to maintain the security and integrity of the system. Each user is responsible for helping toe maintain that security and integrity.

b) Any user who encounters a security problem must repot it immediately to the Technology Director or Building Principal. Do not attempt to repeat the problem or to identify the source.

(Continued)

SUBJECT: INTERNET/COMPUTER USE STANDARDS (Cont'd)

Monitoring of District Internet Users

The District provides access to the Internet for authorized instructional, personnel, business and administrative purposes only. Personal privacy in the use of District Internet facilities and connections will not be guaranteed by the Alexander Central School District. In an attempt to assure that the District Internet facilities and connections are being used only for authorized purposes, the District may:

a) Limit usage of facilities and connections to assigned times and/or locations.

b) Require users to sign a log or to execute log-in procedures to create a record of their usage.

c) Use software or other electronic means to monitor individual usage.

d) Examine all personal electronic files.

Loss of Internet Privileges

Any person who violates the District Internet Policy, practices and procedures or the terms of the user agreement will have his/her Internet privileges revoked, suspended or modified.

a) Students. A student's privileges will be revoked, suspended or modified by the Building Principal. The Building Principal shall promptly notify the student and parents as necessary. The student and parents shall have the right to an informal conference with the Building Principal to discuss the basis of the action taken. The decision of the Building Principal may be appealed to the Superintendent. A student's conduct on the Internet which would be a violation of the District student discipline code may result in disciplinary action in addition to a revocation, suspension or modification of Internet privileges. Any such disciplinary action must be taken in accordance with the applicable due process of law and District policy, practices and procedures.

b) Employees. An employee's privileges will be revoked, suspended, or modified by the employee's supervisor. Any employee's conduct on the Internet which would warrant disciplinary action in addition to a revocation, suspension or modification of Internet privileges, must be take in accordance with the applicable due process of law, bargaining unit agreements, and District policy, practices and procedures.

Adopted: 7/10/02
Updated: 1/6/16

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING POLICY

In compliance with the Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the District has adopted and will enforce this Internet safety policy that ensures the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students. The District will provide for the education of students regarding appropriate online behavior including interacting with other individuals on social networking Web sites and in chat rooms, and regarding cyberbullying awareness and response. Further, appropriate monitoring of online activities of minors, as determined by the building/program supervisor, will also be enforced to ensure the safety of students when accessing the Internet.

Further, the Board of Education's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the schools including the selection of appropriate teaching/instructional materials and activities to enhance the schools' programs; and to help ensure the safety of personnel and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided to ensure compliance with the CIPA.

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web *may* include, but shall not be limited to, the following guidelines:

a) Ensuring the presence of a teacher and/or other appropriate District personnel when students are accessing the Internet including, but not limited to, the supervision of minors when using electronic mail, chat rooms, instant messaging and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of e-mail, chat rooms, as well as social networking Web sites, may be blocked as deemed necessary to ensure the safety of such students;

b) Monitoring logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors;

c) In compliance with this Internet Safety Policy as well as the District's Acceptable Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and

d) Appropriate supervision and notification to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal identification information regarding such students.

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING POLICY (Cont'd.)

The determination of what is "inappropriate" for minors shall be determined by the District and/or designated school official(s). It is acknowledged that the determination of such "inappropriate" material may vary depending upon the circumstances of the situation and the age of the students involved in online research.

The terms "minor," "child pornography," "harmful to minors," "obscene," "technology protection measure," "sexual act," and "sexual contact" will be as defined in accordance with CIPA and other applicable laws/regulations as may be appropriate and implemented pursuant to the District's educational mission.

**Under certain specified circumstances, the blocking or filtering technology measure(s) may be disabled for adults engaged in bona fide research or other lawful purposes. The power to disable can only be exercised by an administrator, supervisor, or other person authorized by the School District.*

The School District shall provide certification, pursuant to the requirements of CIPA, to document the District's adoption and enforcement of its Internet Safety Policy, including the operation and enforcement of technology protection measures (i.e., blocking/filtering of access to certain material on the Internet) for all School District computers with Internet access.

Internet Safety Instruction

In accordance with New York State Education Law, the School District may provide, to students in grades K through 12, instruction designed to promote the proper and safe use of the Internet. The Commissioner shall provide technical assistance to assist in the development of curricula for such course of study which shall be age appropriate and developed according to the needs and abilities of students at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the Internet.

Under the Protecting Children in the 21st Century Act, students will also be educated on appropriate interactions with other individuals on social networking Web sites and in chat rooms, as well as cyberbullying awareness and response.

Access to Inappropriate Content/Material and Use of Personal Technology or Electronic Devices

Despite the existence of District policy, regulations and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access such content or material from their home, other locations off school premises and/or with a student's own personal technology or electronic device on school grounds or at school events.

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING POLICY (Cont'd.)

The District is not responsible for inappropriate content or material accessed via a student's own personal technology or electronic device or via an unfiltered Internet connection received through a student's own personal technology or electronic device.

Notification/Authorization

The District's Acceptable Use Policy and accompanying Regulations will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet.

The District has provided reasonable public notice and has held at least one (1) public hearing or meeting to address the proposed Internet Safety/Internet Content Filtering Policy prior to Board adoption. Additional public notice and a hearing or meeting is not necessary when amendments are made to the Internet Safety Policy in the future.

The District's Internet Safety/Internet Content Filtering Policy must be made available to the FCC upon request. Furthermore, appropriate actions will be taken to ensure the ready availability to the public of this policy as well as any other District policies relating to the use of technology.

The Internet Safety/Internet Content Filtering Policy is required to be retained by the school for at least five (5) years after the funding year in which the policy was relied upon to obtain E-rate funding.

47 United States Code (USC) Sections 254(h) and 254(l)
47 Code of Federal Regulations (CFR) Part 54
Education Law Section 814

NOTE: Refer also to Policy #7315 -- Student Use of Computerized Information Resources (Acceptable Use Policy)
District Code of Conduct on School Property

Adoption Date: 7/10/02
Updated: 1/20/10; 1/6/16