EDUCATIONAL TECHNOLOGY USE

I. Philosophy

The Board of Education is committed to optimizing student learning and teaching effectiveness. The Board considers access to a computer network, including the Internet, to be a powerful and valuable educational and research tool and encourages the use of computers and computer-related technology for the purpose of advancing and promoting learning and teaching.

The district's technology resources include, but are not limited to, computer networks and connections, the resources, tools and learning environments made available by or on the networks, and any and all devices provided by the district that connect to those networks.

II. Expectations for Use of School District Technology

All users of the district's technology resources, including its computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. This policy applies to all district provided technology resources, regardless of whether the use of such resources occurs on or off school property.

All users are responsible for demonstrating appropriate conduct on the school's computer network. Individual users are responsible for their behavior and communications when using those resources or when willfully allowing others to use them. The district reserves the right to control access to the Internet for all users of its computers and network. The district may either allow or prohibit certain kinds of online activity and/or access to certain websites.

The Superintendent is authorized to develop and implement regulations consistent with this policy. All users of the district's computer network and equipment shall comply with this policy, regulations, and general school rules governing student conduct and behavior. Failure to comply may result in legal action and/or disciplinary action including, but not limited to revocation of computer privileges and/or suspension.

III. Terms and Conditions for Use of District Technology

All users of the district's technological resources, including its computer network and the Internet are required to maintain respectful, responsible and appropriate use of technology resources. Responsible use of technological resources is use that is ethical, respectful, academically honest and supportive of student learning.

Prohibited Activity and Uses

1. Users shall not send electronic communications fraudulently (i.e., anonymously or knowingly misrepresenting the identity of the sender).
2. Users shall not attempt to learn or utilize the passwords of other users or network administrators, nor shall users share their own password or the passwords of other users with any other individual(s).
3. Users shall not attempt to gain unauthorized access to the network including, but not limited to, developing or using programs to infiltrate the system or alter software of hardware on the network.
4. Users shall not read, delete, copy or modify or attempt to read, delete, copy or modify the emails or files of other users (except that administrators do have the right to access files, Internet, e-mail, etc., for the purpose of updating and monitoring district technology resources).
5. Users shall not copy or modify server or network system files.
6. Users shall not utilize system resources for illegal activities, or in support of illegal activities. Users must comply with all applicable laws, including, but not limited to those related to copyrights and trademarks, confidential information, and public records.
7. Users shall not utilize the district's technological resources for purposes of engaging in discrimination, harassment, bullying and/or cyberbullying as prohibited by these policies, regulations, the District Code of Conduct and the Dignity for All Students Act.
8. Users shall not violate copyright law or infringe on any copyrights or other intellectual property rights by engaging in activities including, but not limited to, making copies of any licensed programs, installing or using any Internet-based file sharing programs designed to facilitate unauthorized sharing of copy righted materials, and/or copying, transmitting, installing, receiving, transmitting or making available any copyrighted software on the district's network.
9. Users shall not take credit for resources found while utilizing the Internet. When using electronic databases or the Internet for research, all users are expected to properly document all information retrieved. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism as stated in the district's Code of Conduct.
10. All users are expected to remain within allocated disk space. Users must purge, delete or eliminate electronic mail or outdated files that unnecessarily take up excessive storage space on a regular basis.
11. Users shall not use anonymous proxies to circumvent the district's content filtering.
12. Users shall not willfully attempt to alter any district imposed settings utilized to manage student and staff information, technology accounts or usage.
13. Users shall not engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics, (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

14. Users shall not use or view inappropriate language when using the internet or e-mail via the network. Inappropriate language includes, but is not limited to: profanity, vulgarity, impolite or abusive language, ethnic or racial slurs, sexually oriented and/or any other inflammatory language that is prohibited by these policies, regulations and/or the Code of Conduct.
15. Users shall not employ the network for personal or commercial purposes.
16. Users shall not download or install any commercial software, shareware, or freeware onto network drives or disks. Users shall not install their own software on district computers or networks without authorization from an administrator.
17. Users of school district technology resources shall respect school district property and be responsible when using the equipment. Users shall not abuse computer or network hardware. Users shall not attempt to destroy, damage, disable or otherwise interfere with district equipment or materials, delete data or degrade or disrupt system performance. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for the district's technological resources under their control.
18. The district is responsible for any routine maintenance or standard repairs to district resources.
19. Users are responsible for making backups of any data files stored on the local hard drive.
20. Users shall report missing, damaged or malfunctioning hardware or software to the appropriate school administrator.
21. Users who identify a security problem on the district's network shall notify the appropriate school administrator.
22. Users shall not engage in vandalism. Vandalism is defined as any malicious attempt to alter or destroy the data of another user, provider, or any agencies or other networks that are connected to the Chittenango Central School District network. This includes, but is not limited to, the uploading or creation of computer viruses.

IV. Actions to Discourage Inappropriate Use

School administrators and staff including, but not limited to, teachers, library media specialists and support personnel shall take the following actions to discourage inappropriate use of the Internet:

1. Use passwords to limit Intranet access to authorized users only.
2. Require users to change their password on a regular basis.
3. Require that district personnel closely supervise students using the district's technological resources in order to guide them towards appropriate materials and uses in accordance with this policy.
4. Filter Internet connections.
5. Educate students about appropriate online behavior.
6. Impose sanctions for policy violations.

V. Remote Access and Use of Personal Technology

Remote access to district networks or proprietary information is a privilege. Persons with those privileges have the responsibility to safeguard it from any unauthorized user or person not entitled to access of confidential information. Remote users are subject to all of the terms and conditions set forth in these policies, regulations and the district Code of Conduct.

Users shall not connect any personal technologies to the district's network without permission from the school principal. Such permission may be granted only for educational purposes. Users of personal technology are subject to all of the terms and conditions set forth in these policies, regulations and the district Code of Conduct.

Students and staff who are issued district-owned hardware such as laptop computers or computer tablets are responsible for the proper maintenance and use of said hardware. Users of such hardware must agree to the following terms:

1. Keep the device secure and damage free. Use the protective case at all times.
2. Do not leave the device unattended.
3. Do not leave the device in a vehicle or outside.
4. Do not use the laptop near pets or near water such as a sink, tub, toilet or pool.
5. Do not remove or attempt to remove any marking which denotes the device as district property.
6. Do not loan out the device or related materials.
7. Do not load or attempt to load any non-educational software or software application onto the device without the expressed consent of a school administrator.

VI. Internet Safety

The Board of Education is committed to undertaking efforts to make the use of district technology for access to the Internet safe for children. The district is unable to guarantee that any selected filtering and blocking technology will work perfectly; however, the Superintendent of Schools shall procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children’s Internet Protection Act.

Subject to staff supervision, any such measures may be disabled or relaxed for adults conducting bona fide research or for other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using email, chat rooms, and other forms of direct electronic communications, monitoring the online activities of students using district computers, and restricting student access to materials that are harmful to minors.

Child pornography means 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: (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (b) 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 (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Harmful to minors 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 as to minors.

VII. Privacy

All users of the district's technological resources, including its computer network and the internet, shall have no expectation of privacy with regard to the use of any hardware, software, electronic mail (e-mail) or other computer equipment owned or leased by the Chittenango Central School District. The district reserves the right to access and view any materials stored on district equipment or any material used in conjunction with the district's computer network. Administrators may review files and communications to examine their contents in order to maintain system integrity, and to ensure that users are using the system appropriately and responsibly.

VIII. Sanctions

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Violations of this policy by students and/or district personnel shall be reported to the building principal. The principal shall take appropriate action in accordance with authorized disciplinary procedures as set forth in these policies and the district Code of Conduct. Sanctions may include, but are not limited to, suspension and/or revocation of computer access privileges.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to, materials protected by copyright, threatening or obscene material or material protected by trade secrets. Users must respect all intellectual and property rights and laws.

IX. Unauthorized Disclosure of Personally Identifiable Information

Personally identifiable information concerning minors may not be disclosed or used in any way on the Internet (e.g., on the district web page or otherwise) without the permission of a parent or guardian in accordance with provisions of the Family Educational Rights and Privacy Law Act ("FERPA"). If a student is 18 years of age or older, the permission may come from the student himself/herself.

The Board prohibits the unauthorized disclosure, use and dissemination of personally identifiable information regarding students, teachers or principals. Students and staff may not use any cloud-based educational software or application without first obtaining approval from the appropriate district administrator. The administrator will determine if the terms of service of the software or application are sufficient to address the Education Law's privacy and security requirements, or whether parental permission or a formal contract with the software or application provider is required.

X. Policy Dissemination

The Superintendent, through his designees, is responsible for disseminating the policy and associated regulations to school personnel, students and parents annually.

Adoption Date: June 4, 2002
Effective Date: July 1, 2002
Revised: May 18, 2004, December 12, 2014, March 17, 2015

Ref: Public Law No. 106-554
Education Law § 2-d
47 USC §254
20 USC §6801