SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES

The Churchville-Chili Central School District provides technology resources to its students solely for educational purposes. 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.

In accordance with the Children's Internet Protection Act, the District installs and operates filtering software to limit user's Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, the District cannot guarantee that filtering software, as explained in the Internet Safety Policy 8271, does not negate or otherwise affect the obligation of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

The District's electronic network is intended to support the educational program and is not a public forum for general use. Student users may access technology for only educational purposes. The actions of student users accessing networks through the District reflect on the District; therefore, student users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Students are responsible for their behavior and communications using the Districts computers and networks.

(Continued)

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (CONT'D)

Standards of Acceptable Use

Student users of technology will:

- Use or access District technology only for educational purposes
- Comply with copyright laws and software licensing agreements. Torrenting any copyrighted material is illegal and not allowed through the district network. Students are not allowed to stream music and/or movies from any site that does not prove it has a legal licensing agreement with the copyright holder.
- Understand that email and network files are not private. Network administrators may review files and communications to maintain system integrity and monitor responsible student use.
- Respect the privacy rights of others.
- Be responsible at all times for the proper use of technology, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords.
- Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.
- Abide by the policies and procedures of networks and systems linked by technology.

Students may not use District technology for improper uses. These uses include, but are not limited to:

- Any and all illegal purposes, these include, but are not limited to spreading computer viruses, arranging for drug sale, purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.;
- Any and all obscene or pornographic purposes, including, but not limited to, retrieving or viewing sexually explicit material;
- Any and all discriminatory purposes, including harassment and bullying of individuals based on race, gender, religion, sexual orientation, or disability, among others;
- Any and all purposes that would violate state, federal or international law, including
  - Copyright laws;
  - Cyberbullying laws; and
  - Sexting laws.
- Any use of profanity, obscenity, or language that is offensive, harassing or threatening;
- Reposting or forwarding personal communications without the author's prior consent;
- Reposting or forwarding of junk mail, chain letters, or inappropriate or offensive jokes;

(Continued)

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (CONT'D)

Standards of Acceptable Use (Cont'd)

Improper uses (cont'd.), but are not limited to:

- Destruction, alteration, disfigurement or unauthorized access of hardware, software, or firmware;
- Obtaining financial gain or Transacting any business or commercial activities;
- Plagiarizing (claiming another person's writings as your own);
- Political advocacy;
- Disrupting the use of others to any process, program or tool, including downloading or otherwise spreading computer viruses;
- Engaging in hacking of any kind, including, but not limited to, the illegal or unauthorized access;
- Allowing others to use Property issued under the program without authorization, including students whose access privileges have been suspended or revoked;
- Soliciting or distributing information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.

The use of computerized information resources is a privilege, not a right. 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 Student Discipline 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.

No Expectation of Privacy

Users should not expect that email or files stored on District servers will be private. The District reserves the right to log technology use, to monitor fileserver space utilization by users, and to examine users' files and materials as needed, and at its discretion. Users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside the District.

(Continued)

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (CONT'D)

Internet Safety

Students must take steps to ensure their safety on the internet, including, but not limited to, the following rules:

- Students should never give out identifying information such as home address, school name, or telephone number to others on the Internet or by email, including in a public message such as chat room or newsgroups. If a person asks for such personal information, it should be reported to a teacher, administrator and/or parent immediately.
- Students should not post photographs of themselves in newsgroups or on websites that are available to the public.
- Students should not arrange a face-to-face meeting with someone they "meet" on the Internet or by email.
- Student Users should not respond to messages that are suggestive, obscene, belligerent, threatening, or make a student user feel uncomfortable. If a student receives such a message, he or she should provide a copy of the message to a teacher, administrator and/or parent immediately. If the message requires school action (e.g., bullying) the student's parent should provide a copy to the a CCCSD administrator.
- Use of anonymizers, proxy servers and VPN connections to bypass the district content filter is prohibited. Use of these sites put you and your personal data at risk, bypassing the safety measures the district has in place to protect your online activity.

The District recommends that parents/guardians read and follow the U.S Department of Justice Guidelines for Parents/Guardians on Internet Safety located at: https://www.justice.gov/criminal-ceos/children-internet-safety

Notification/Authorization

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. Student access to the DCS will automatically be provided unless the parent has submitted written notification to the District that such access not be permitted. Procedures will be established to define the process by which parents may submit a written request to deny or rescind student use of the DCS in accordance with law, Commissioner's Regulations and/or District policies and procedures.

(Continued)

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (CONT'D)

Consequences for Unacceptable Use

Violations of this policy, or any administrative regulations and guidelines governing the use of technology, may result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion, or other appropriate disciplinary action. Violations of local, state or federal law may subject students to prosecution by appropriate law enforcement authorities.

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

Adopted: 7/10/2001
Revised: 1/09/2007, 10/25/2011, 3/25/2014, 7/10/2018
Reviewed by Superintendent, Assistant Superintendent for Instruction and Director of Information Technology on 10/21/2021 with no recommended changes; BOE agreed & approved 11/9/2021