SUBJECT: INTERNET ACCESS AND ACCEPTABLE USE POLICY FOR STUDENTS, FACULTY AND STAFF/INTERNET CONTENT FILTERING

We are pleased to offer the students, faculty and staff of the Tully Central School District use of the latest in computer technology hardware and software as well as access to the Internet and the World Wide Web.

Families should be aware, however, that some material available via the Internet and World Wide Web may contain things that are not age-appropriate and could be potentially offensive, defamatory, inaccurate or even illegal.

Independent use of the computers at Tully is a privilege, not a right. Independent access is defined as access that is not under DIRECT teacher supervision and that is for any purpose other than access to web-delivered course content assigned by a teacher (e.g. classroom support sites and District-purchased web-delivered electronic materials). This privilege may be, and will be, revoked or denied as a result of improper account holder behavior. System administrators may deny independent access at any time as required. The administration, faculty and staff at Tully Central School District as well as parents/guardians may request the System Administrator to deny, revoke or suspend such independent access.

a) Prior to access to the Internet, training will be given in both its use and etiquette ("netiquette").

b) Users are expected to treat computers, other hardware peripherals and software with respect. Failure to do so will be considered misuse/abuse. This includes, but is not limited to:

1. Placing/installing personal software or information on District workstations without the expressed permission of the System Administrator;

2. Placing/installing unlawful information on District workstations;

3. Willfully destroying District property, stored information and/or system programs/software;

4. Accessing and/or using obscene, abusive or otherwise objectionable text, sounds or images;

5. Downloading unauthorized information to workstations, fileservers or diskettes;

6. Ignoring rules of cleanliness in workstation work areas (e.g. no food or drink spills)

d) Users are to protect their passwords at all times. The network is intended for the exclusive use of its registered users, who are responsible for the use and security of their passwords and accounts. ANY PROBLEMS WHICH ARISE FROM MISUSE OF A USER'S ACCOUNT ARE THE RESPONSIBILITY OF THE ACCOUNT HOLDER. Any misuse of password security, such as a person using another person's account, will result in the immediate suspension of

(continued)

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

account privileges for one or both parties involved in the misuse.

d) Account holders should understand that District-supplied Electronic Mail is not secure and can be read by others.

e) Student, Faculty and Staff data files and electronic storage areas shall remain the property of Tully Central Schools, subject to District control and inspection. The system administrator may access all such files and communications to insure system integrity and that users are complying with the requirements of this policy.

f) All communications and information collected via the Internet are assumed to be private property and must be properly cited by users, as would any other copyrighted material.

g) In order to support the vision and mission of the Tully Central School District, the district may maintain a website for the following purposes.

1. As a place to showcase innovative student and staff educational projects, presentations, and learning experiences;

2. As a gateway to a district and community resources and educational websites that support the instructional goals of the District;

3. A method for community members to access district information and publications;

4. A means of communications to and from students, district personnel, the community and associated organizations.

(a) All web authors (students, faculty or staff) must participate in training to familiarize themselves with appropriate and acceptable website posting procedures. Failure to follow the outlined regulations and procedures may result in the loss of authoring privileges or more stringent disciplinary measures.

(b) Documents may not contain objectionable material or link to objectionable material. Objectionable material is defined as text, images, sounds, etc. of obscene, abusive or violent nature, or any materials not directly congruent with the purpose and mission of the Tully Central School District. Web pages must also be adhere to copyright laws.

(c) Where feasible, links to non-district supported services should contain a disclaimer indicating that the user is leaving the District server and that the District does not necessarily approve the linked material. Web pages on the District's server are the property of the District. The web server may be examined periodically to check for the timelines and relevance of its pages.

(continued)

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

(d) Safeguards for the Students:

1) Web pages may include only the first name and initial of the last name of any student. Pages or filenames may not include a student's phone number, address, Email address or names of other family members, friends and/or relatives.

2) Use of individual student pictures (video/still) and audio clips on the District web page must have signed parent/guardian approval on file for the students under 18 years of age. Group pictures (video/still), audio clip, etc may be published without parent/guardian approval if names are omitted.

3) Teachers who have students create web pages must use due diligence to monitor the student work on these web pages for appropriate content.

Internet Content Filtering

The Tully Central School District, in accordance with the provisions of the Children's Internet Protection Act, requires all District computers with Internet access that are used by elementary and secondary students and staff to be equipped with filtering or blocking technology.

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:

(continued)

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

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, ~~and~~ 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.

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.

(continued)

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

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.

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.

Consequences for the Misuse/Abuse of District Property and/or the Internet

Depending on the severity of the misuse, the disciplinary process may include combinations of the following:

a) Verbal warning

b) Written warning and parental notification

c) Referral to Building Principal

d) Loss of email and Internet accounts

e) Possible criminal charges

(continued)

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

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: 04-02-2012