SUBJECT: STUDENT USE OF COMPUTER INFORMATION RESOURCES (ACCEPTABLE USE GUIDELINES)

Program Implementation

The Onondaga Central School District Board of Education recognizes the world uses technology to manipulate information in many ways ranging from gathering, recording, constructing knowledge, demonstrating, problem-solving and collaborating. The district is committed to supporting Computer Assisted Instruction as an important educational tool for students to utilize the resource of technology to enhance their learning. Consequently, the School System 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 "Internet." The District shall provide personnel support for such usage.

The District’s Computer System is for educational and/or research use only and must be consistent with the strategic goals and mission of the Onondaga Central School District. The standards of acceptable use as well as prohibited conduct by students accessing the DCS, as outlined in District policy and regulation, are not intended to be all-inclusive. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. In addition to the specific standards of student conduct delineated in this regulation, the general requirements of acceptable student behavior expected under the District's school conduct and discipline policy and the Code of Conduct also apply to student access to the DCS. Communications on the network are often public in nature. General school rules for behavior and communications apply.

Legal and ethical implications of software use will be taught to students of all levels where there is such software use. In addition, the building principal or his/her designee and/or classroom teacher will be responsible for informing District students of rules and regulations governing student access to the DCS.

Access to the District’s computer network is for educational purposes which include classroom activities, career development, curriculum development and communication. As much as possible, access to the District's computerized information resources will be designed in ways which point students to those resources that have been reviewed and evaluated prior to use. While students may be able to move beyond those resources to others which have not been evaluated by staff, students shall be provided with guidelines and lists of resources particularly suited to the learning objectives.

(continued)

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

Standards of Conduct Governing Student Access to District’s Computer System

Inappropriate use of the DCS may result in disciplinary action, including suspension or cancellation of access. Prior to suspension or revocation of access to the DCS, students will be afforded applicable due process rights. Each student who is granted access will be responsible for that usage. The DCS is provided for students in support of their educational program and to conduct research and communicate with others. Student access to external computer networks not controlled by the District is provided to students who act in a considerate and responsible manner. Individual users of the District's computerized information resources are responsible for their behavior and communications over the District computer network. It is presumed that users will comply with District standards and will honor the agreements they have signed.

A student is responsible for keeping a log of all contacts made on the District's computer network. The full Internet address of each correspondence on the network must be included in this log. A count of all mail received must be included in this log. The District computer coordinator or his/her designee will be responsible for placing a log book near each computer capable of accessing the network.

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 Director of Technology may access all such files and communications to insure 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 District’s Computer Network will be private.

During school, teachers will guide students toward appropriate materials. Outside of school, parents/guardians bear responsibility for such guidance as they do with information sources such as television, telephones, movies, radio, video games, cell phones and other potentially offensive/controversial media.

Use of the DCS which violates any aspect of Onondaga Central School District policy; the Code of Conduct; and federal, state or local laws or regulations is strictly prohibited and may result in disciplinary action in compliance with applicable District guidelines and/or federal, state and local law including, but not limited to, suspension and/or revocation of access to the DCS. In addition to the District's general requirements governing student behavior, specific activities shall be prohibited by student users of the DCS including, but not limited to, the following:

(Continued)

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

1) Do not engage in defamation, do not employ another’s password or disclose user information or user information that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or Internet.

2) Do not upload or disseminate viruses or Trojan horses or other harmful form of programming or vandalism; do not participate in hacking activities or any form of unauthorized access to other computers, networks, or information systems.

3) Using the DCS to obtain, view, download, send, print, display or otherwise gain access to or to transmit materials that are unlawful, obscene, pornographic or abusive

4) Use of obscene or vulgar language.

5) Damaging, installing, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.

6) Using unauthorized software on the DCS.

7) Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the student without express permission from the Director of Technology.

8) Illegal activities, including violating copyright law or contract violations as well as tampering with computer hardware or software that includes any and all devices such as keyloggers.

9) Employing the DCS for non-educational, commercial purposes, product advertisement, political lobbying, financial or religious purposes.

10) Transmitting material, information or software in violation of any District policy or regulation, the District Code of Conduct, and/or federal, state and local law or regulation.

11) Revealing personal information about oneself or of other students including, but not limited to, disclosure of home address and/or telephone number.

(Continued)

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

12) No user is permitted to knowingly or inadvertently load or create a computer virus or load software that destroys files and/or programs and disrupts network performance.

13) Appropriate behavior is expected while on or near school property, in school vehicles (including school buses and vans) and at school sponsored activities.

14) Students may not use the DCS to sell or buy anything or the Internet.

15) The use of proxy software or proxy services to get around content filtering is prohibited and is a direct violation of this agreement, sites prohibited are all social networking sites including but not limited to myspace, facebook, xanga.

16) Appropriate language should be used in all communications. The student should not participate in "Cyberbullying" which is to torment, threaten, harass, humiliate, embarrass or otherwise target a child, preteen or teen using the Internet, interactive and digital technologies or mobile phones through direct attacks (messages sent directly) or by proxy (using others to help cyberbully the victim, either with or without the accomplice's knowledge). Direct Attacks include: Instant Messaging/Text Messaging Harassment, stealing passwords, blogs, websites, sending pictures through email or cell phones, internet polling, interactive gaming, sending malicious code, sending porn and other junk email and instant messages, impersonation.

17) Misuse of computer/electronic communication, including any unauthorized use of telephones, two-way radios, multifunction cell phones, mp3 players, ipods, jamming/interference devices, video games, computers, peer to peer networks, software, or internet/intranet accounts, email or instant messaging accounts, disruption or access to security systems hardware or software.

Use of Web 2.0 Technologies and Tools

Known as the read and write technology. Web 2.0 is web-based services and tools that make content creation on the web easier and more accessible to a group. These technologies are user centered, offer multimedia experiences and are innovative. Access and exploration of these communication and collaborative tools is critical to our student's success in the 21st century. These tools provide authentic, real world collaboration and offer a vehicle to manipulate information in many ways ranging from gathering, recording, constructing knowledge, demonstrating, problem-solving and collaborating. Expectations for classroom blogs, wikis, podcasts or other web interactive use must follow all established Internet safety guidelines and Acceptable Use policies.

(Continued)

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

1. Use of blogs, podcasts or other web 2.0 are considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom or school bus is also inappropriate in all uses of web 2.0 technologies.
2. Students using blogs, podcasts, or other web tools are expected not to divulge personal information online.
3. A student should never post personal information on the web, no names, photographs, addresses and should never agree to meet someone you have met via the Internet.
4. Students who do not follow the terms and conditions in this policy or those set forth by your classroom teacher may lose the opportunity to use the selected technologies as part of the classroom project and may be subject to the consequences of inappropriate use.

Network accounts are to be used only by the authorized owner of the account. Any user of the DCS that accesses another network or computer resources shall be subject to that networks acceptable use policy.

If a student or a student's parent/guardian has a District network account, a non-district network account or any other account or program which will enable direct or indirect access to a District computer, any access to the DCS in violation of District policy and/or regulation may result in student discipline. Indirect access to a District computer shall mean using a non-district computer in a manner which results in the user gaining access to a District computer, including access to any and all information, records or other material contained or stored in a District computer.

Sanctions

1) Violations may result in suspension and/or revocation of student access to the DCS as determined in accordance with appropriate due process procedures.

2) Additional disciplinary action may be determined at the building level in accordance with existing practices and procedures regarding inappropriate language or behavior, as well as federal, state and local law.

3) When applicable, law enforcement agencies may be involved.

(Continued)

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

Security

Security on any computer system is a high priority, especially when the system involves many users. Users of the DCS identifying a security problem on the District's system must notify the teacher in charge. A student is not to demonstrate the problem to other users. Attempts to log on to the DCS as a computer administrator both on the domain or locally may result in restriction or suspension of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the DCS. Further, any violations regarding the use and application of the DCS shall be reported by the student to the teacher in charge.

Notification/Authorization

Only those students who have signed an agreement form and provided written permission from parents/guardians may access the DCS (affirmative consent to opt-in), including potential student access to external computer networks not controlled by the School District. Permission is not transferable and may not be shared. All required forms must be kept on file in the District Office. (Refer to Forms #7314F and #7314F.1).