SOMERS CENTRAL SCHOOL DISTRICT

Acceptable Use Policy Guidelines
For Students and For District Employees

I. PURPOSE

The Board has adopted Acceptable Use and Internet Safety Policies to set forth its policies for access to Somers Central School District (SCSD) electronic telecommunication systems. The Policies provided for the development of regulations and guidelines for use of the telecommunication systems by students and staff. Telecommunication systems are herein defined as any electronic device or network accessible technology used to communicate or convey audio, text, or visual messages. The following rules and regulations have been developed to implement Board policy.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student access to the district electronic telecommunication systems the district considers its own stated educational mission, goals and objectives. Access to and use of telecommunication systems has become a powerful tool for promoting educational excellence by facilitating research, information delivery, sharing, innovation, communication, productivity and learning. While these tools have become vital to communication and information access not all material is suited for the K-12 environment. The district expects that faculty will blend thoughtful use of the schools telecommunication systems and the Internet throughout the curriculum and will provide guidance and instruction to students on their safe and appropriate use.

III. LIMITED EDUCATIONAL PURPOSE

Somers Central School District provides employees and students with access to its telecommunication systems. The purpose of these systems is not general access but has a more specific limited educational purpose. This purpose includes use of telecommunication systems for professional SCSD business, classroom instructional activities, professional and career development and to further educational and personal goals consistent with the school district mission, goals, and objectives and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on these limited purpose systems.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the SCSD telecommunication system is a privilege not a right. Depending on the nature and degree of the violation and the number of previous violations unacceptable use of the district's telecommunication systems or the Internet may result in one or more of the following consequences to be meted out pursuant to applicable laws, policies or agreements that may exist: suspension or cancellation of use of access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

V. USER ROLES AND RESPONSIBILITIES

It is the responsibility of any individual using SCSD telecommunication systems to read, understand, and follow these policy guidelines. In addition, users are expected to exercise reasonable judgment in interpreting these guidelines and in making decisions about the appropriate use of SCSD resources. Any person with questions regarding the application or meaning of this policy should seek clarification from the appropriate teacher or school administrator. Use of SCSD resources shall constitute acceptance of the terms of these policy guidelines.

A. SCSD ADMINISTRATOR ROLES AND RESPONSIBILITIES

Every SCSD administrator is responsible for being knowledgeable about acceptable use and online safety issues. Administrators are responsible for their own safe and appropriate use of the telecommunication systems and must abide by Section VI herein. Additionally, each administrator is also responsible for making certain that the faculty, staff, and students in their respective school facility or department understand and abide by the Somers Central School District Internet Safety Policy and Acceptable Use Policy. If a SCSD administrator has reason to believe that a user, whether it be faculty, staff, or student, is misusing the systems, the administrator has the right to request that the individual's account and access be reviewed. It is also the responsibility of the administrator to report to the Superintendent or his/her designee any misuse of SCSD telecommunication systems and resources.

B. SCSD TEACHER ROLES AND RESPONSIBILITIES

Each SCSD teacher is responsible for being knowledgeable about acceptable use and online safety issues. Teachers are responsible for their own safe and appropriate use of the telecommunication systems and must abide by Section VI herein. Additionally, each teacher who uses SCSD telecommunication systems with students is responsible for teaching their students about safe and responsible use of networked environments and telecommunication systems including the intranet and Internet and integrating this training into their respective instructional areas. Teachers are responsible for monitoring student activity while online and while using SCSD resources to make sure they are using them appropriately. Teachers should make sure that students understand acceptable use and abide by the terms of acceptable and unacceptable use as defined in this document (Section VI). If a teacher has reason to believe that a student is using these resources inappropriately, it is the right to request that the individual's account and access be reviewed. It is also the responsibility of the teacher to report any misuse of SCSD telecommunication systems and resources to the appropriate building or department administrator.

C. SCSD NON-CERTIFIED STAFF ROLES AND RESPONSIBILITIES

All non-certified staff (e.g., clerical, support staff, etc.) are responsible for their own safe and responsible use of networked environments and telecommunication systems including the intranet and Internet. It is the responsibility of each non-certified staff member to understand and abide by the terms of acceptable and unacceptable use as defined in this document (Section VI). It is the responsibility of non-certified staff to assist teachers and administrators, whenever possible, to report students and staff they have reason to believe are using these resources inappropriately.

D. SCSD OTHER STAFF ROLES AND RESPONSIBILITIES

All other staff members, including Library Media Specialists, School Resource Officers, and Information Services staff hold the same level of rights and responsibilities as school teaching staff. However they have the added responsibility of being the point persons for working with and training all administrators, teachers, and non-certified district staff in network and online safety and appropriate use of available telecommunication systems resources. As such they have the responsibility to remain current about new technologies and potential issues related to network and online safety. They have a right to intervene whenever they have reasonable suspicion that staff or students are misusing SCSD systems by suspending access to the respective system until it is reported to and investigated by the appropriate school or district personnel.

E. SCSD STUDENT ROLES AND RESPONSIBILITIES

It is the responsibility of students using SCSD telecommunication systems to learn about safe and responsible use of networked environments and telecommunication systems including the intranet and Internet. Students are responsible for using these resources appropriately. They must abide by the terms of acceptable and unacceptable use as defined in this document (Section VI). If a student misuses SCSD telecommunication systems, administrators and teachers in the district must report it to the Superintendent or his/her designee.

F. PARENT/GUARDIAN ROLES AND RESPONSIBILITIES

The roles and responsibilities of parents and guardians are described elsewhere in this document. To review these roles and responsibilities see Section XIII.

VI. ACCEPTABLE AND UNACCEPTABLE USES

A. The SCSD telecommunication systems including the intranet and Internet are to be used for educational purposes.

B. The telecommunication system allows for access to social media sites. Student users acknowledge that the SCSD provides age-appropriate instruction regarding appropriate interaction with others via e-mail, on social networking sites, and in chat rooms as well as cyberbullying awareness and response to cyberbullying and they agree to conduct themselves appropriately when using SCSD technology.

C. It is unacceptable to use SCSD telecommunication for:
    1. posting or reposting private, personally identifiable information about another person without permission (including, but not limited to, home address), except for District personnel who are authorized to release directory information pursuant to the District's FERPA policy; telephone numbers, identification numbers, account numbers, access codes or passwords, photographs, height, weight);
    2. sending threatening or harassing messages;
    3. making or transmitting false, defamatory, or libelous statements about another person, group, or organization;
    4. accessing or sharing pornographic, sexually explicit, obscene, or otherwise harmful or inappropriate materials for minors;
    5. gaining or attempting to gain unauthorized access to SCSD computer and telecommunication systems;
    6. interfering with the daily operation of SCSD computer and telecommunication systems, including knowingly placing a computer virus on or within any computer or telecommunication system;
    7. accessing or attempting to access another person's account, password, or files without prior implied or direct consent of that person;
    8. intercepting communications intended for another person without prior authorization;
    9. engaging in any commercial or fundraising purpose without authorization from the appropriate school district official;
    10. furthering any political or religious purpose;
    11. engaging in any illegal act or violate any local, state, or federal statute or law;
    12. downloading, uploading, or distributing any files, software, or other material in violation of federal copyright laws or intellectual property laws;
    13. attempting to gain unauthorized access to the school district's systems or any other system through the school district's telecommunication systems;
    14. violating software usage or licensing agreements; and
    15. offering or providing goods or services or for product advertisement or to purchase goods or services for personal use.

D. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school official. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. A user may also in certain rare instances access otherwise unacceptable materials if necessary to complete an assignment and if done with prior approval of, and with appropriate guidance from, the appropriate teacher.

E. Those employees with access to data of students, parents and/or other employees shall not be shared outside of the confines of normal job functions.

F. Reporting of Violations
    1. Violations of the Internet Safety Policy, the Acceptable Use Policy and/or these regulations by students and/or staff shall be reported to the Building Principal.
    2. The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures and the Code of Conduct.

VII. MONITORING INTERNET ACCESS

A. With respect to any computers within Somers Central School District with Internet access, the school district will monitor the online activities of minors, employees, and guests. The district will employ technology protection measures during any use of such computers by minors and adults, including, but not limited to firewalls, filters, bandwidth monitoring, and shaping tools, antivirus software, anti-spyware software and pop-up blockers. The technology protection measures utilized will block access to material or visual depictions on the Internet and World Wide Web that are:
    3. Obscene
    4. Child pornography; or
    5. Harmful to minors.

B. The term "child pornography" refers to 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:
    1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
    2. 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
    3. Such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
C. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
    1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
    2. Depicts, describes, or represents, in any 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
    3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
D. An administrator, supervisor, or other person authorized by the Superintendent/Director of Technology shall be responsible for ensuring the installation and proper use of any Internet monitoring, blocking and filtering technology protection measures used by the district.
E. An administrator, supervisor, or other person authorized by the Superintendent/Director of Technology may disable the technology protection measure, during the use by an adult, to enable access for bona fide research or other lawful purposes.
    1. The access of any adult staff for whom the technology protection measures have been disabled shall be monitored to ensure that there is not access to materials or visual depictions that are child pornography or otherwise obscene.
F. An administrator, supervisor, or other person authorized by the Superintendent/Director of Technology shall monitor student online activities to ensure all users, including but not limited to students, are not engaging in "hacking" (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

VIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the district's telecommunication shall be consistent with school district's mission, goals, objectives and policies as well as the varied instructional needs, learning styles, abilities and developmental levels of its students. The district's network and related computer systems are not a public forum. Violations of the Internet Safety Policy, Acceptable Use Policy and these guidelines by students may result in discipline pursuant to the SCSD's Code of Conduct and/or appropriate legal action. Any violation of the Internet Safety Policy, Acceptable Use Policy and these guidelines by staff may result in discipline pursuant to applicable New York State Law and/or a collective bargaining agreement, as well as appropriate legal action.

IX. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school district's telecommunication systems the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal data or files on the school district equipment or systems.
B. An administrator, supervisor, or other person authorized by the Superintendent/Director of Technology may inspect, copy, review and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and electronic communications, as well as any and all information transmitted or received during such use.
C. Routine maintenance and monitoring of the school district systems may lead to a discovery that a user has violated this policy, another school district policy, or law.
D. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

E. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual accounts at any time.
F. School district employees should be aware that data and other materials in files maintained on the school district systems may be subject to review, disclosure, or discovery under federal and state statutes, including, but not limited to, the Family Educational Rights and Privacy Act of 1974 (FERPA).
G. The school district will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities and activities not in compliance with school district policies conducted through the school district's systems in accordance with the law.

X. INTERNET USE AGREEMENT

A. The proper use of the Internet and the educational value to be gained from proper Internet use is the joint responsibility of students, parents, and employees of the school district.
B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.
C. The Internet Use Agreement form must be read and signed by the user (if able to sign or if entering grade four or above) and the parent or guardian. The form must then be filed at the school office (students and school staff) or at the user's respective department office (non-school based employees).

XI. USE OF PERSONAL EQUIPMENT AND DEVICES

To the extent that a student or staff use their own device or equipment on school property, the device or equipment is subject to the same monitoring and/or review as SCDS devices and/or equipment if the SCDS administration has reason to believe that such device or equipment is being used to violate the Acceptable Use Policy or its guidelines. Additionally, the use of personal equipment or devices using the SCSD network will subject the device and/or equipment to monitoring and/or review of such usage.

XII. LIMITATIONS ON SCHOOL DISTRICT LIABILITY

Use of the school district's telecommunication systems including the intranet and Internet is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including but not limited to loss, damage or unavailability of data stored on school district storage media, including but not limited to diskettes, tapes, hard drives, jump drives, or servers, or for delays or changes in or interruptions of service or mis-deliveries or non-deliveries of data, information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district's systems. The school district will not be responsible for financial obligations arising through unauthorized use of the school district's systems, including the intranet and Internet.

XIII. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to telecommunication systems use.
B. This notification shall include the following:
    1. Notification that intranet and Internet use is subject to compliance with school district policies.
    2. Disclaimers limiting the school district's liability relative to
        a. Information stored on school district magnetic media, including but not limited to diskettes, hard drives, jump drives or servers.
        b. Information retrieved through school district computers, networks, or online resources.
        c. Personal property used to access school district computers, networks, or online resources.
        d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.
    3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
    4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this Acceptable Use Policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student or the student's parents/guardians.
6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Family Educational Rights and Privacy Act of 1974 (FERPA).
7. Notification that should the user violate the school district's acceptable use policy, the student's access privileges may be limited, suspended, or revoked. In addition, school disciplinary action may be taken and/or appropriate legal action may be taken given the severity of the offense.
8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XIII. PARENT RESPONSIBILITY – NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media. Parents are responsible for monitoring their students' uses of the school district systems and of the Internet if the students are accessing the school district systems from home or a remote location.
B. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:
    1. A copy of the user notification form provided to the student user.
    2. A description of parent/guardian responsibilities.
    3. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and a supervising teacher prior to use by the student.
    4. A statement that the school district's acceptable use policy is available for parental review.

XIV. IMPLEMENTATION AND POLICY REVIEW

A. The school district's Internet Safety Policy, Acceptable Use Policy and these guidelines are available for review by all parents, guardians, staff, and members of the community.
B. Because of the rapid changes in the development of the Internet the school district shall conduct an annual review of the Acceptable Use Policy and these guidelines.

XV. SCSD ONLINE SAFETY PROGRAM

SCSD staff members, are provided network and online safety instruction on an ongoing basis. This training is provided in one or more of the following ways:

A. nationally recognized online training (e.g., i-Safe, NetSmartz, etc.);
B. SCSD sponsored professional staff development (online and face-to-face);
C. national, regional, and local presentations by recognized Internet safety organizations and law enforcement agencies (e.g., Operation Blue Ridge Thunder, i-Safe, etc.);
D. ad hoc one-on-one mentoring, training, and model teaching (primarily conducted by other staff – Information Services, Library Media Specialist, and School Resource Officers);
E. national, state, and local workshops, symposia, and conferences and online resources made available through SCSD web site.
F. Training to students is provided as part of the regular instructional program and is integrated into the classroom lessons where appropriate.
G. Training to parents of students is provided through online sources, local organizations, and the individual school parent-teacher association (PTA).

XVI. DISCLAIMERS

The Somers Central School District make no warranties of any kind, either expressed or implied, for SCSD telecommunication systems resources including the intranet or Internet. SCSD are not responsible for any damages incurred, including but not limited to loss of data resulting from delays or interruption of service, loss of data stored on SCSD resources, or damage to personal property used to access SCSD resources; for the accuracy, nature, or quality of information stored on SCSD resources or gathered through SCSD intranet or the Internet; or for unauthorized financial obligations incurred through SCSD-provided access. Furthermore, even though SCSD may use technical or manual means to limit student access these limits do not provide a foolproof means for enforcing the provisions of this policy. All provisions of this agreement are subordinate to local, state, and federal statutes.

This policy is in compliance with local, state, and federal telecommunications rules and regulations.