Sunapee School District	GBEF-R

SCHOOL DISTRICT ACCEPTABLE USE POLICY FOR STAFF

Computer information systems and the abundant sources of information available on the internet greatly enhance the quality of education available to all students. Therefore, use of computers, networks, electronic sources and access to the Internet will be made available to students and staff in the Sunapee School District for the purpose of conducting research, communicating with others for educational purposes, exchanging information and ideas, and as an audience for student writing and a natural environment for collaborative work.

Purpose of this document

To establish a policy to ensure efficient, safe, ethical and legal use of the Sunapee District's computer information systems. These policies apply to all users of computer information systems located or accessed in the District as well as users who obtain their access privileges through associations with the District.

Definition

The definition of "computer information systems" is any configuration of computer hardware and software that connects users. This includes all internal (intranet) and external (Internet) connections, as well as all of the computer hardware, operating system, software, application software, stored texts and data files. This also includes electronic mail, local database, externally accessed databases, CD-ROM, recorded magnetic or optical media, clip art, digital images, digitized information, portable communication technologies, and new technologies as they become available. Stand-alone workstations are also governed by this agreement.

Educational Purpose

The Sunapee School District provides resources for teaching and learning, communication services, and business data services by maintaining access to local, regional, national, and international sources of information. Members of the school community will use the Sunapee School District computer information resources with respect for the public trust that they have been provided and in accordance with policy and regulations established by the Sunapee School District. Only authorized students and staff may use School District information networks, and the network shall not constitute a public forum. This policy/agreement does not attempt to articulate all required and prescribed behavior by computer information system users.

Successful operation of the computer information systems requires that all users conduct themselves in a responsible, decent, ethical and polite manner while using the computer information systems. The user is ultimately responsible for his/her actions in accessing the computer information systems.

The District will endeavor to provide a safe and wholesome Internet environment. However, it is possible that a user will be able to find ways to circumvent Internet access limits and controls. For that reason, parents will be warned of the potential availability of offensive material on the Internet, and students and parents will both be advised that the student is ultimately responsible for his/her own conduct on the Internet. The written permission of parent/guardian is required before students may use the School District's computer information systems. The permission must be updated yearly.

Responsibilities

Computer use is a privilege and not a right. Every user accepts the responsibility to respect the rights of all other computer/network users and to act in a responsible, polite, ethical and legal manner at all times.

Students are responsible for proper behavior on school computers and networks just as they are in the classroom. General school rules for behavior and communications apply. Because in-school computer access is a privilege, and because each user is personally responsible for his or her own actions, unacceptable behavior may result in the suspension or revocation of computer/network and/or Internet access.

Staff are responsible for following the school board policy pertaining to staff ethics (GBC), staff conduct (GBCB), staff-student relations (GBH).

Levels of Access

Computer and Electronic Resources: Access to computers gives students an opportunity to use a wide range of electronic resources in their class work and research, explore their own interests, and pursue independent study. All students have access to computers and electronic resources.

Internet: All computers district wide have been set up for Internet use. All students, with parental approval, may use the World Wide Web to search for information, save or print text files, download images, format documents and computer programs with faculty permission and guidance.

E-mail: Some students are issued email accounts for educational purposes.

Monitoring and Data Retention Policy

1. Network administrators may review files and communications to maintain system integrity and ensure that users have used or are using the system responsibly.
2. All log files used by the School District for monitoring purposes generally will be purged from the system 90 days after the file creation data. These will include all logs currently generated by the Proxy server in all schools and the SAU office.
3. All log files and files created on the servers are considered School District Property.

Acceptable Use

1. Access to the computer information systems within the District is a privilege and must be treated as such by all users.

2. Computer information systems will be used only for the purposes of academic research, education, and school-related business and operations. Computer information systems may not be used for recreational, personal or commercial purposes.
3. Any system which requires password access or for which the District requires an account will only be used by the authorized account user. Account owners are ultimately responsible for all activity under their accounts.
4. The resources of the District are limited. All users must exercise prudence in the shared use of this resource.
5. All communications and information accessible via any District computer information system shall be treated as School District property.
6. All software used on District equipment must be licensed to the district.
7. All software installation will be done by District authorized personnel only.
8. Use of non-district computers on district network is not allowed.

Unacceptable Use

The District has the right to take disciplinary action, remove computer and networking privileges and/or take legal action, for any activity characterized as unethical and unacceptable. Unacceptable activities constitute, but are not limited to, any activity through which any user:

Violates such matters as institutional or third party copyright, license agreements or other contracts. The unauthorized use of and/or copying of software is illegal.

Interferes with or disrupts other network users, services or equipment. Disruptions include, but are not limited to: distribution of unsolicited advertising, propagation of computer worms or viruses, distributing quantities of information that overwhelm the system, and/or using a District network to make unauthorized entry into any other resource accessible via the network.

Seeks to gain or gains unauthorized access to information resources.

Uses or knowingly allows another to use any computer or computer system to devise or execute a scheme to defraud, obtain money, property, services, or other things of value by false pretenses, promised or representations.

Destroys, alters, dismantles or otherwise interferes with the integrity of computer based information and/or information resources.

Invades the privacy of individuals or entities.

Uses the information systems for commercial or political activity.

Destroys, modifies or abuses the hardware or software in any way.

Installs unauthorized software for use on District computers.

Modifies computer configuration settings including but not limited to screen resolution, desktop patterns/pictures, file sharing configurations, printers and network settings without prior authorization of the Technology Coordinator.

Uses the computer information systems to access inappropriate materials.

Acquires, communicates, creates, submits, publishes, displays or participates in any defamatory, inaccurate, racially orientated, offensive, abusive, obscene, pornographic, profane, sexually -orientated, illegal, harassing, vandalizing, violent, inappropriate or threatening materials, messages or activities on a District computer information system.

Notwithstanding the District's right to retrieve and monitor any e-mail messages, such messages should be treated as confidential by other employees and students and accessed only by the intended recipient. Employees and students are not authorized to retrieve or read any email that is not sent to them. Any exception to this policy must receive prior approval by the superintendent.

Violating school policies and standards of behavior or any other illegal activities including copyright violation and unauthorized access to restricted materials.

Sending, downloading, storing, printing, or displaying files or messages that are profane, obscene, offensive or harassing.

Damaging computer systems or disrupting network users, services or equipment.

Using computers or networks for personal, financial or commercial gain.

Submitting a copy or revision of another file, if represented exclusively as your own work.

Creating, reproducing, or revising a file for use by another student, when that file is represented exclusively as your own work.

Unauthorized entry into computers, changing or destruction of computer files, tampering or changing computer hardware/software, or altering computer/network operating environments, or other vandalism.

Using the school's Internet connection for any illegal activity, including copyright violation.

Disrupting or interfering with network users, services, or equipment, including (but not restricted to) sending chain letters or broadcasting messages to multiple lists or individuals.

Using the school's Internet connection to access Internet Relay Chat (IRC) and unsupervised interactive games.

Users are not to reveal, forward, or publicize identifying information (name, personal address, phone number) of themselves or others.

User is solely responsible for an assigned account. The responsibility for security of files is yours. Under no conditions should you give your password to anyone. If another student gains access to your files, even if unauthorized by you, and submits a copy of your work, you could be held responsible.

Students should be aware that all on-line sessions can be monitored and those site names visited are recorded and the log is periodically checked. It is to be noted that the system administrator has access to all files. The administrator reserves the right to log and monitor network use and file server space by users. The administrator assumes no responsibility or liability for deleted or damaged files due to violation of fileserver space allotments.

Restricted Materials and Actions

To keep users safe and our information systems secure, the following is NOT allowed:

No use of personal email accounts. Users may not access these accounts from the school network. This includes, but is not limited to Hotmail, AOL mail, Yahoo mail, and personal mail accounts through an Internet Service Provider account.

No use of peer-to-peer file sharing programs. Examples of this would be sites such as Sharaza, Limewire or Kazaa.

No use of Instant Messaging, including, but not limited to AOL Instant Messenger, MSN Messenger, ICQ, and Yahoo Messenger, unless specifically authorized by the Technology Coordinator.

No use of online games, unless for educational purposes.

No use of chat rooms unless specifically authorized by the Technology Coordinator. Authorization will be for one session only and must be requested if access is needed after the first session.

No downloading and/or storage of illegal MP3 files or Gaming files on District equipment.

For students: Disclosure of personal contact information such as name, address, or phone number. Do not give out any personal information except for academic purposes such as college applications and scholarships. Never arrange to get together with someone you meet online.

For web pages: No use of student's full name, address or email address in conjunction with a photograph.

Do not respond to any illicit or suspicious activities, and immediately report them to a School District administrator.

Consequences of Violations

The Sunapee School District values the appropriate and responsible use of its computer information systems. Any system user identified as a security risk or violating district computer guidelines will face consequences that may include denial of access to the District's system. A violation of any of the rules and guidelines outlined in this agreement will result in the following consequences:

Faculty consequences
Infractions set forth in this agreement may result in suspension or termination of access privileges and/or appropriate disciplinary action in accordance with district policy and collective bargaining agreements. Inappropriate behavior in violation of state and federal statues will be subject to prosecution by those authorities.

The District reserves the right to:

1. Monitor all activity.
2. Make determinations on whether specific uses of a network are consistent with network usage guidelines.
3. Log network and monitor disk space utilization by users.
4. Determine what is appropriate use.
5. Remove a user's access to the network at any time it is determined that the user engaged in unauthorized activity or violated acceptable use procedures.
6. Cooperate fully with any investigation concerning or relating to the District's network activity.

7. Read, review, audit, intercept, access or disclose any and all information on an employee's or student's computer system any messages created, received or sent over the electronic mail system for any purpose, even if coded or password protected without prior notice.

Sunapee School District Internet Safety Policy

Internet Resources

The Internet is a global computer network of schools, libraries, businesses, governments, organizations and millions of individuals all exchanging or publishing ideas and information. Access to the Internet will enable students to explore thousands of libraries, databases and bulletin boards while exchanging messages and ideas with Internet users throughout the world. The Internet includes outstanding government and scientific information, as well as valuable material on business, current events, the arts and popular culture. Its resources change constantly and are not always authoritative or accurate.

Because the Internet is largely unregulated, not all the information it carries is suitable for school children. During school, teachers will guide students toward appropriate materials and insofar as possible, monitor students' use. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials. Within reason, freedom of speech and access to information resources and opportunities for collaboration far exceed any of these disadvantages. To gain access to the Internet, all students under the age of 18 must obtain parental permission.

Recognizing that the resources of the internet are becoming more and more important as an educational resource, and noting that at the same time the internet's content is broad and unrestricted, the Sunapee School District wishes to assure that Sunapee students and staff have ready access to the internet, while minimizing the risk of accidental or purposeful contact with inappropriate material.

We are required, and intend, to comply with Title XVII Children's Internet Protection and assure that the school district:

A. has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are
   a obscene
   b child pornography; or
   c harmful to minors; and
   d is enforcing the operation of such technology protection measure during any use of such computers by minors; and
B. has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are
   a. obscene; or
   b child pornography; and

In addition we wish to assure that our students are provided with appropriate guidance as they use the internet for research, cooperative learning, etc.

Therefore, it shall be the policy of the Sunapee School District to:

a prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

b prevent unauthorized access and other unlawful online activity;

c prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

d comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "internet filters") shall be used to block or filter internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. No filter is more than 60% effective at blocking access to inappropriate material. Therefore, no K-5 student shall use the internet except when under the direct supervision of a school staff member. Grades 6-8 may have less supervised access in computer labs and the library. Grades 9-12 require less direct supervision.

We recognize that human supervision cannot assure that continuous observation is possible; therefore, we will provide an internet proxy server with a commercially available filtration system which will be used to filter all internet access from any computer in the Sunapee School District. Access will be controlled through the proxy server. Filtering will be imposed on a graduated basis. There will be increasingly restrictive levels of filtration with administrators, and teachers having the fewest restrictions and K-5 students the most. This filter may also be used to filter other inappropriate material beyond that included in CIPA as directed by the administrators of each building (i.e. Drugs, Alcohol, Games, etc.).

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. From time to time, the filter may block sites which are appropriate for legitimate educational use. In those cases, the staff member shall make a request to the helpdesk to have the block removed.

Additionally, each student is responsible for following the Acceptable Use Policy (AUP) (which is included in the Parent/Student Handbook). These responsibilities include maintaining appropriate network and computer use. To the extent practical, steps shall be taken to promote the safety and security of users of the Sunapee School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communication.

Specifically, as required by the Children's Protection Act, prevention of inappropriate network usage includes:

(a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and

(b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Additionally, use of instant messaging by minors to communicate with anyone outside the district without a specific waiver (i.e. exchange student communication, communication as part of an online class) is specifically forbidden.

This is monitored both directly and through periodic, online spot checks of student and staff use. Violations of the AUP may have consequences ranging from a request to change sites, a direction to discontinue computer use for the balance of the period, loss of internet access privileges, loss of computer privileges, detention, and/or suspension.

We look forward to the continued integration of the internet into the education of our children. We want to use this material to provide a broader view of the world consistent with our mission. A continued careful approach to internet safety will assure that the best possible use of the internet will continue.

Appendix:

Technology Protection Measure- The term technology protection measure means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of Title 18, United States Code;
2. Child Pornography, as that term is defined in section 2256 of Title 18, United States Code; or
3. Harmful to Minors. The term 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.
4. Sexual Act; Sexual Contact. The terms sexual act and sexual contact have the meanings given such terms in section 2246 of Title 18, United States Code.

I understand and agree to the above.

Signature____________________________________Date_______________________

First Reading: August 7, 2013
Second Reading and Approval: November 6, 2013