SCHOOL DISTRICT ACCEPTABLE USE POLICY FOR STUDENTS

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.

As a school district we are committed to preparing students to be positive, caring, and contributing members of society by maintaining high academic, social, and civic expectations within a secure environment. We strive to provide access to technology in order to enhance students' ability to problem solve effectively, read effectively, write effectively, speak well, and demonstrate knowledge and skills, in keeping with our Vision of the Graduate. In using technology, we expect that students will act with courtesy, respect, integrity, and compassion, demonstrate responsibility and initiative, both as independent learners and as team members, and be helpful and contribute to the school and community.

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.

Definitions

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.

The terms Computer, Computer Information Systems, and District-owned device refer to any electronic device that can access the Internet or communicate with any other device. This includes but is not limited to personal computers, tablets, streaming media players, etc. that are owned by Sunapee School District.

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 terms sexual act and sexual contact have the meanings given such terms in section 2246 of Title 18, United States Code.

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;

2. 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

3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. (This section was moved up from Appendix which only contained this section. Now all definitions are in the Definitions section.)

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 proscribed 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 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 District-owned devices and networks just as they are in the classroom, during and outside of school hours. Students are responsible for proper care and charging of District-owned Chromebooks or other devices issued to them for use at home. 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 device/network access, Internet access, and/or other consequences listed below.

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 District-owned devices 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 District-owned devices 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 use computer programs with faculty permission and guidance.

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

Monitoring and Data Retention Policy

I. 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 date.

3. All log files and files created on the servers are considered School District Property.

4. All District-owned devices are monitored by District staff while the devices are on District networks. Student devices can be monitored when used at home. Devices are monitored during regular school hours Monday – Friday when school is in session, in-person or remote. Issues identified during other days and times will be addressed the next school day, whether in- person or during remote learning.

4a. Monitoring consists of one or more of the following:

- Live real time view of the student's screen by designated staff members;
- Record of browsing history such as a list of sites visited by the student;
- Record of sites the student attempted to view but were blocked by content filtering;
- Review of student email or other communications;
- Automated alerts by monitoring software that detects inappropriate communication or possible danger signals such as threatening messages sent or received.

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 these resources.

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 will be installed by District authorized personnel only.

8. Use of non-District computers on District internal networks is not allowed.

9. District-owned devices must be brought to school fully charged each day and protected from damage. Removing protective covers or decorating with stickers or other items is not allowed.

Unacceptable Use

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

1. 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.

2. 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 or District-owned device to make unauthorized entry into any other resource.

3. Seeks to gain or gains unauthorized access to information resources.

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

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

6. Invades the privacy of individuals or entities.

7. Uses the information systems for commercial or political activity.

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

9. Installs unauthorized software for use on District–owned devices.

10. Modifies lab computer or loaner device configuration settings including but not limited to screen resolution, desktop patterns/pictures, file sharing configurations, printers and network settings on a District-owned device without prior authorization of the Technology Director, except when modified as an accessibility accommodation.

11. Uses the computer information systems to access inappropriate materials.

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

13. Violates school policies and standards of behavior or commits any other illegal activity including copyright violation and unauthorized access to restricted materials.

14. Sends, downloads, stores, prints, or displays files or messages that are profane, obscene, offensive or harassing.

15. Damages computer systems or disrupts network users, services or equipment.

16. Uses District-owned devices or networks for personal, financial or commercial gain.

17. Submits a copy or revision of a file, if represented exclusively as the student's own work. Creating, reproducing, or revising a file for use by another student, when that file is represented exclusively as the student's own work.

18. Logs into computers without authorization, changes or destroys computer files, tampers with or changes computer hardware/software, or alters computer/network operating environments, or commits other vandalism.

19. Uses the school's Internet connection for any illegal activity, including copyright violation. Disrupts or interferes with network users, services, or equipment, including (but not restricted to) sending chain letters or other media, or broadcasting messages to multiple lists or individuals.

20. Uses the school's Internet connection to access chat rooms or 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 other than a teacher or District administrator. 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.

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.

Students should be aware that all on-line sessions can be monitored and the names of sites 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:

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

2. No use of peer-to-peer file sharing programs without staff permission.

3. No use of the TOR network or the "dark web".

4. No use of Instant Messaging unless specifically authorized by the Technology Director.

5. No use of online games, unless for educational purposes and approved by a teacher.

6. No use of chat rooms.

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

8. No use of Virtual Private Network (VPN) software.

9. No 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.

10. Never arrange to get together with someone you meet online.

11. No use of student's full name, address, email address, photograph, or other personally identifiable information entered into a web site or other online resource, other than school tools that have passed the data privacy law's vetting process.

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

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 systems. A violation of any of the rules and guidelines outlined in this agreement will result in the following consequences:

Student consequences
First infraction may result in any of the following: afterschool detention, Saturday detention, removal from the computer information systems for one to five school days, restriction from taking Chromebook or other device home, Digital Citizenship education, notification sent to parent. Such notification will require parental signature before access is re-established.
Second infraction may result in any of the following: one or more afterschool detentions, Saturday detention, removal from the computer information systems for one to fifteen consecutive school days, restriction from taking Chromebook or other device home, Digital Citizenship education, notification sent to parents. A student, parent, and staff conference is required before access will be re-established.
Third infraction may result in any of the following: one or more Saturday detentions, removal from the computer information systems for one to thirty consecutive school days, restriction from taking Chromebook or other device home, Digital Citizenship education. Notification sent to parents. A student, parent, and staff conference is required before access will be re- established.
Subsequent infractions: removal from the computer information systems for one to forty-five consecutive school days, restriction from taking Chromebook or other device home, Digital Citizenship education. Notification sent to parents. A student, parent, and staff conference is required before access will be re-established.
Note 1: accelerated consequences may be applied at the discretion of the administration in any case, regardless of whether or not it is a first, second, third, or subsequent offense.
Note 2: students will be given one to five days to complete make-up work after privileges have been restored at the discretion of the teacher.

The District reserves the right to:

1. monitor all activity.
2. make determinations on whether specific uses of network resources are consistent with network usage guidelines.
3. log network activity and monitor disk space utilization by users.
4. determine what is appropriate use.
5. remove a user's access to the network or take-home devices at any time it is determined that the user is 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 District-owned device, including any messages created, received or sent for any purpose, even if encrypted or password protected without prior notice.

Internet Resources

The Internet is largely unregulated. Its resources change constantly and are not always authoritative or accurate. Not all the information it carries is suitable for school children. During in-person or remote school, teachers will guide students toward appropriate materials and, insofar as possible, monitor students' use.

Our intent is to make Internet access available to further educational goals and objectives. Within reason, freedom of speech and access to information resources and opportunities for collaboration are very important. Students who want access to a blocked resource should ask their teacher to submit a helpdesk request. If the resource passes vetting or otherwise satisfies legal requirements, the Tech Department will unblock the resource. As noted elsewhere in this policy, all students under the age of 18 must obtain parental permission to gain access to the Internet.

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 ensure 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 Act and ensure that the School District:

1. has in place a policy of Internet safety for minors that includes the operation of technology protection measures with respect to any of its devices with Internet access that protects against access through such devices to visual depictions that are:

    a. obscene;
    b. child pornography; or
    c. harmful to minors.

2. is enforcing the operation of such technology protection measures during any use of such devices by minors.

We are required, and intend to comply with New Hampshire RSA 189:68 Student and Teacher Information Protection and Privacy and ensure that the School District blocks access to websites, extensions and other resources that collect Personally Identifiable Information, have not passed the vetting process, and have not signed the Data Privacy Agreement.

In addition, we wish to ensure that our students are provided appropriate guidance as they use the Internet for research, cooperative learning, etc. Therefore, it shall be the policy of the Sunapee School District to:

1. prevent user access to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications on District-owned devices;
2. prevent unauthorized access and other unlawful online activity on District-owned devices;
3. prevent unauthorized online disclosure, use, or dissemination of personally identifiable information of minors; and
4. comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]. (CIPA)

Access to Inappropriate Material

To the extent practical, technology protection measures (or "content filters") shall be used to block or filter 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.

Filtering is imposed on a graduated basis. There are increasingly restrictive levels of filtration with administrators and teachers having the fewest restrictions and students the most. This filter

may also be used to filter other inappropriate material beyond that included in CIPA as directed by District administration (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

No filter is more than 60% effective at blocking access to inappropriate material. Therefore, no K-5 student shall use the Internet on District-owned devices except when under the direct supervision of a school staff member or parent/guardian at home. Grades 6-8 may have less supervised access. Grades 9-12 require still less direct supervision.

Additionally, each student is responsible for following this Acceptable Use Policy (AUP) which is included in the Parent/Student Handbook. These responsibilities include maintaining appropriate network and device use. To the extent practical, steps shall be taken to promote the safety and security of users of the Sunapee School District computer network.

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

1. unauthorized access, including so called "hacking"" and other unlawful activities; and

2. 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 device use for the balance of the period, loss of Internet access privileges, loss of device privileges, loss of take-home Chromebook or other device, detention, and/or suspension as described earlier in this document.

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 ensure that the best possible use of the Internet will continue.

Please consider very carefully your decision to withhold any item of personally identifiable information. Should you decide to inform the School District not to release any or all of the items listed below, any future requests for such information from individuals or entities not affiliated with the School District will be refused. This would include scholarship information, news releases, college transcripts, etc.

Information to be withheld: _____

_____

_____ Yes, I will allow my child's picture, video or sound recording to be published on the school website.

_____ No, I will not allow my child's picture, video or sound recording to be published on the school website.

If this form is not received by the School District by_____**(Date),** it will be assumed that the above information may be released for the remainder of the current school year. A new form for non-release must be completed each year.

Student's Name: _____

Parent's Name: _____

Parent's Signature:_____ Date: _____

Signature

Adopted by the Sunapee School Board at their October 2011 school board meeting. This policy remains in effect until amended or revoked.

First Reading: August 7, 2013
Second Reading & Approval: November 6, 2013
Revised: April 22, 2021
First Reading: May 5, 2021
Second Reading & Approval: June 2, 2021