

Acceptable Use of the Internet and Internet Safety Policy

REGULATION #5132-R

ACCEPTABLE USE OF THE INTERNET AND OTHER ELECTRONIC COMMUNICATION SYSTEMS FOR STUDENTS

Computers and networks provide access to resources as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users; respect the integrity of the system and related physical resources; and observe all relevant laws, regulations, and contractual obligations. Use of computers by students and access by students to computer networks and to the Internet are services made available only to further the educational mission of the Stamford Public Schools. In order to be granted these access privileges and to retain them, students must abide by the guidelines set forth in the Board's "Acceptable Use of the Internet and other Electronic Communication Systems for Students" policy and these regulations at all times when they use the Stamford Public Schools systems. These computer systems are expensive to purchase, install and maintain. As the property of the district these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, access to the computer systems is a privilege, and not a right. Students under the age of 18 may use electronic information retrieval systems in supervised settings and only with the written permission of a parent or guardian through a duly executed "Acceptable Use Agreement." Stamford students may use the district's electronic information retrieval systems provided they:

- Abide by the Acceptable Use Policy
- Sign an "Acceptable Internet Use Agreement"
- Obtain the signature of a parent/guardian (for students under the age of 18)

Any parent or student inquiry regarding any decision relative to Stamford's Acceptable Use Policy and/or these administrative regulations should be directed to the District Internet Administrator.

Information Networks:

The Stamford Public Schools' network connects all of the schools and offices. This makes sharing of information and communicating with all schools and offices possible. This network supports activities that have educational value for administration, instruction and learning by teachers and students. The Internet is a collection of many worldwide networks that support the open exchange of information. The Internet provides immediate access to information anywhere in the world.

Student Behavior:

Students are expected to use all computer equipment, both hardware and software and network access to pursue intellectual activities, to seek resources, to access libraries and for other types of learning activities. They will learn new things and can share their new found knowledge with classmates, teachers, parents and global learning partners. For the safety of all involved, caution must be exercised.

Because the Stamford Public Schools' network is used as part of a school activity, the policy on student behavior applies to network activity. Therefore, the Acceptable Use Policy is an extension of the district's Policy on Student Behavior. These rules apply to vandalism of computer equipment, unauthorized access to information, computer piracy, hacking, tampering with hardware and software, bullying and harassment. Conduct including, but not limited to, the following, is prohibited with respect to use of these computer systems:

- Sending any form of harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime, pursuant to Public Act 95-143, and other laws);
- Gaining or seeking to gain unauthorized access to computer systems;
- Damaging computers, computer files, computer systems or computer networks;
- Using another person's password under any circumstances;
- Trespassing in or tampering with any other person's folders, work or files;
- Sending any message that breaches the district's confidentiality requirements, or the confidentiality of students;
- Sending any copyrighted material over the system. In addition, as noted above, if a particular behavior or activity is generally prohibited by law or by Board policy or school rules or regulations, it must not occur in the use of these computer systems.
- Deliberately accessing, creating, displaying transmitting, or otherwise possessing or disseminating material that contains pornography, obscenity, sexually explicit, or indecent/inappropriate language, text, sounds, or pictures.

Improper behavior may result in disciplinary penalties, including but not limited to, loss of computer privileges, suspension and/or expulsion.

Copying Software:

With a few exceptions, software on the Stamford Public Schools' computers and network are licensed for use on the Stamford Public Schools' computers only. Copying software from a computer or network is prohibited unless specifically authorized in writing by an appropriate authority. *In addition to disciplinary penalties imposed by the Stamford Public Schools, illegal copying of software is subject to civil damages and criminal penalties, including fines and imprisonment.*

Moral and Ethical Issues:

The Stamford Public Schools wants to provide a stimulating educational environment in which students, teachers, and parents can grow as a learning community. While the Stamford Public Schools want this valuable educational tool used, the use of inappropriate information on the Internet will not be condoned. Some materials exist which are inappropriate to the instructional setting, and reasonable measures will be taken to prevent them from being accessed. Users must clearly understand that access to such material in any form is strictly forbidden. The network is designed to achieve and support instructional goals and is not intended to be used for financial gain. Any information that does not support classroom learning should be avoided. Although the actual percentage of unacceptable materials is small, it can cause concern for students and parents if a student accesses those materials while doing legitimate research. If a student has a question or concern regarding any materials found, students should apprise the teacher. The Stamford Public Schools has in place the state recommended web filtering software to minimize the risk to student. However, filtering software is not 100% effective; while filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. It is the user's responsibility not to initiate access to materials that are inconsistent with the goals, objectives and policies of the educational mission of the District.

Electronic Libraries:

Materials on the Internet can be considered part of a vast digital library. Electronic database and information search tools to access the Internet are part of school media centers and libraries. Guidelines for access to information have already been established in the Library Bill of Rights of 1980. These principles can be applied to the Internet as well. This document states that "attempts to restrict access to library materials violate the basic tenets of the Library Bill of Rights"; however, school librarians are required to devise collections that are "consistent with the philosophy, goals and objectives of the school district." This means that students have the right to information, but the school has the right to restrict any information that does not apply to the approved curriculum.

Student Email:

Students will be issued a district-owned email account which is the sole property of Stamford Public Schools. All email activities must comply with the Acceptable Use Policy. The user accepts all responsibility to understand the policy. The primary purpose of the student email system is for students to communicate with school staff and fellow students to collaborate on school activities. Use of the school's email system is a privilege. Students are responsible for messages and material stored and sent from their email accounts. Students should not share their passwords. The email system should be used for education purposes only and cannot be used to operate personal business. Students should have no expectation of privacy. The district reserves the right to retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages, to conduct internal investigations, to comply with investigations of wrongful acts or to recover from system failure.

Virtual Field Trips:

The information networks offer many opportunities for "virtual field trips" to distant locations. The Stamford Public Schools consider all connections to remote locations as "virtual field trips." Rules that apply to student conduct on field trips apply to "virtual electronic field trips" as well. It is important that students realize that they represent their school and their school district when they use information networks, and are expected to be on their best behavior.

Monitoring

It is expected that students will comply with district standards and will act in a responsible and legal manner at all times, in accordance with district standards, state and federal laws. It is important that students and parents understand that the district, as the owner of the computer systems, intends to monitor and review the use of these computer systems in an effort to ensure that users engage only in appropriate uses. As part of monitoring and reviewing, the district will retain the capacity to bypass any individual password of a student or other user. The system's security aspects, such as personal passwords and message delete function for E-mail, can be bypassed for these purposes. The district's ability to monitor and review is not restricted or neutralized by these devices. The monitor and review process also includes oversight of Internet site access, review of email and of document downloading and printing.

Therefore, all users must be aware that *they should not have any reasonable expectation of personal privacy in the use of these computer systems.*

In addition, the Stamford Public Schools accept the requirements of the Children's Internet Protection Act (CIPA). Accordingly, each district computer with Internet access shall have a filtering device that blocks entry to visual depictions that are obscene, pornographic or harmful or inappropriate for students, as defined by CIPA and as determined by the Superintendent or his/her designee. The Superintendent or his/her designee shall make arrangements to enforce the use of such filtering devices. Administrators or other authorized personnel may disable the filtering device for legitimate pedagogical research or for any other lawful purpose, provided such person obtains prior approval from the Superintendent or his/her designee. Filtering should be viewed as only one of a number of techniques used to manage students' access to the Internet and to encourage acceptable usage. Filtering should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors.

Filtering should be used in conjunction with:

- Educating students concerning the dangers of inappropriate material on the Internet;
- Using recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
- Using the district's "Acceptable Use" agreement;
- Using behavior management practices for which Internet access privileges can be earned or lost; and
- Appropriate supervision, both in person and/or electronically.

Internet Safety:

Students are expected to conduct themselves in an appropriate manner at all times when they use or interact with any of Stamford Public Schools' hardware and software resources. This includes, but is not limited to, interaction with district computers, email communication, web browsing software, or even usage of one's own personal hardware over a district network connection.

To help ensure student safety and citizenship in online activities, all students will be educated about appropriate behavior, including interacting with other individuals on social networking websites, collaborating using web 2.0/3.0 tools, instant messaging, video messaging, chat rooms, and cyber-bullying awareness and response.

This policy is a component of the district's responsibility to create and maintain a safe, civil, respectful, and inclusive learning community and shall be implemented in conjunction with comprehensive training of students, staff and volunteers.

The district will provide students with strategies aimed at preventing harassment, intimidation, and bullying. In its efforts to train students, the district will seek partnerships with families, law enforcement, and other community agencies.

Interventions are designed to remediate the impact on the targeted student(s) and others impacted by the violation, to change the behavior of the perpetrator, and to restore a positive school climate. The district will consider the frequency of incidents, developmental age of the student, and severity of the conduct in determining intervention strategies. Interventions will range from counseling, correcting behavior and discipline to law enforcement referrals.

)

Reporting of Misuse

Anyone who is aware of problems with, or misuse of these computer systems, should report this to his or her teacher or principal immediately. Most importantly, the Board and the administration urge any student who receives any harassing, threatening, intimidating or other improper message through any computer system/communications device, whether district or privately-owned, to report this immediately. Such acts may constitute violations of the district's anti cyber-bullying policy or other policies.

It is the Board's policy that no student should be required to tolerate such treatment, regardless of the identity of the sender of the message. Please report these events!

Use of Personal Electronic Devices:

Connection of any personal electronic device to any network on school grounds is subject to all regulations and guidelines in this document. Students and staff are permitted to connect to the district network via the secure wireless connection provided by the school system, but all access must be in accordance with this Regulation for Acceptable Use of the Internet and Electronic Communication Systems, the School's Student Handbook, and the mission of the school district. Ability for students to use their own devices at school or in a particular class is at the sole discretion of the building administrator and/or classroom teacher. Students are NOT permitted to use their own computing devices to access the Internet via personal Wi-Fi accounts or by any manner other than connecting through the secure wireless connection provided by the school system.

Each user is responsible for his/her personal device and should use it responsibly and appropriately. Stamford Public Schools takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. It is the responsibility of each individual to secure their device when not in use.

Use of Web 2.0/3.0 Tools:

Classroom blogs, wikis, student e-mail, podcasts, Google Apps accounts, online curriculum software/websites or other Web interactive tools must follow all established Internet safety guidelines. Staff and students using blogs, podcasts or other web tools for educational purposes are expected to act safely. Students using such tools agree to not share their username or password with anyone other than their teachers and parents and treat blog spaces and online spaces, or discussion forums, as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog. Users who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences consistent with the district discipline policies.

Regulation Adopted: June 27, 2000.

Amended: June 25, 2002

Amended: July 24, 2012

Amended: April, 2016