Acceptable Use

Introduction

Seneca High School, District #160 (herein referred to as District) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st century technology and communication skills. To that end, we provide access to technology for students and staff use.

This Authorization and Acceptable Use Policy (AUP) does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. All activity over the network or using district technologies may be monitored and retained.

By utilizing district technology equipment, you are agreeing not only to follow the rules in this policy, but are agreeing to report any misuse of the network to the person designated by the school for such reporting. Misuse means any violation of this policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Technologies Covered

The District may provide staff/students with devices such as desktop computers, laptop computers, phones, tablets, hotspots, and more. The District may provide staff/students with services such as Internet Access, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, the District will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available school technologies, not just those specifically listed, and shall also cover the use of personally-owned devices on the school campus.

Internet Safety

Internet access is limited to only those “acceptable uses'' as detailed in these procedures. Internet safety is almost assured if users will not engage in “unacceptable uses,” as detailed in this Authorization, and otherwise follow this Authorization.

Staff members shall supervise students while students are using School Internet access to ensure that the students abide by the Terms and Conditions of Internet access contained in this Authorization. The School District shall endeavor to provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

The District's Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the District. (Note: the filtering device is not guaranteed to block all inappropriate sites. Even the most sophisticated and current technology tools cannot block all inappropriate sites one hundred percent.)

Terms and Conditions

1. Acceptable Use - Access to the District's electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use. The use of the District's electronic network shall: 1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, and developmental levels of the students, and 2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board Policy 6:60, Curriculum Content, students will be educated about appropriate online behavior, including but not limited to 1) interacting with other individuals on social networking websites and in chat rooms, and 2) cyber bullying awareness and response.

The district's electronic network is part of the curriculum and is not a public forum for general use.

Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the district's electronic network. The District's Authorization for Electronic Network Access contains the appropriate use, ethics, and protocol. Electronic communication and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

2. Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or Building administrator will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

3. Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
d. Recognize that email is not private. People who operate the system have access to all email. Messages relating to or in support of illegal activities may be reported to the authorities.
e. Do not use the network in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the network to be school property.

4. Acceptable Use- While working in a digital and collective environment, students should always conduct themselves as good digital citizens by adhering to the following:

a. I will show respect for myself through my actions. I will select online names that are appropriate. I will use caution with the information, images, and other media that I post online. I will carefully consider what personal information about my life, experiences, or relationships I post. I will not be obscene. I will act with integrity.

b. I will ensure that the information, images, and materials I post online will not put me at risk. I will not publish my personal details, contact details, or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me while online. I will protect passwords, accounts, and resources.
c. I will show respect to others. I will not use electronic mediums to antagonize, bully, harass, or stalk people. I will show respect for other people in my choice of websites: I will not visit sites that are degrading to others, pornographic, racist, or inappropriate. I will not enter other people's private spaces or areas.
d. I will protect others by reporting abuse and not forwarding inappropriate materials or communications. I will avoid unacceptable materials and conversations.
e. I will request permission to use copyrighted or otherwise protected materials. I will suitably cite all use of websites, books, media, ect. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.
f. I will request to use the software and media others produce. I will purchase, license, and register all software or use available free and open source alternatives rather than pirating software. I will purchase my music and media and refrain from distributing these in a manner that violates their licenses.

5. **Unacceptable Use** - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
b. Using the network for commercial or private advertising;
c. Using the network for private financial or commercial gain;
d. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
e. Students shall only use their school accounts for district approved software or websites;
f. Wastefully using resources, such as file space;
g. Hacking or gaining unauthorized access to files, resources or entities;
h. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of personal nature;
i. Using the Internet and District resources in any way that would disrupt its use by others;
j. Using another user's device, account or password;
k. Intentionally letting another person use your device, account, or password;
l. Intentionally posting of material authored or created by another;
m. Intentionally posting anonymous messages and/or misrepresenting one's own identity to others;
n. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material. (See Board policy 7:180 Preventing Bullying, Intimidation and Harassment)
o. Capture, record or transmit the words and or images of any student, staff member, or other person in the school without express prior notice and explicit consent.
p. Using the network while access privileges are suspended or revoked and
q. Deleting data, hiding, or attempting to interfere with the discovery of a violation of this policy.
r. Searching the internet off topic/task;
s. Using technology for non-educational purposes.
t. Removal of District software.

6. Cyberbullying – Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Emails or comments sent with the intent of scaring, hurting, humiliating, or intimidating someone else will not be tolerated. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in serve disciplinary action and loss or privileges. Cyberbullying is a crime and authorities will be notified. Remember that your activities are monitored and retained.

7. Personally-Owned Devices Policy – Users must keep personally-owned devices (including laptops, tablets, kindles, smart phones, and cell phones) turned off and put away during school hours – unless in the event of an emergency or as instructed by a teacher or staff for education purposes. When personally owned mobile devices are used on campus, they should only be used over the school guest network unless having express permission from IT staff. The District is not responsible for theft/damages to personal devices.

8. Social Media – We recognize that social media is a way that students connect with the global community, and that it can be used for instruction. Normal school rules of etiquette and conduct spelled out in the student handbook apply to student social media use, including rules applying to bullying and harassment. The school reserves the right to limit or block students accessing such sites via Seneca High School equipment or networks at the discretion of administration.

9. No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user’s errors or omissions. Use of any information obtained via the Internet is at the user’s own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

10. Indemnification – The user agrees to indemnify the District of any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, an breach of this *Authorization*, school policy, or rules and procedures.

11. Security -Network security is a high priority. If the user suspects or can identify a security problem, breach or compromise on the network, the user must notify the system administrator or Building Principal as soon as possible. Do not demonstrate the problem to other users. Account and password information MUST be kept confidential. Using another user’s account without written permission from the administrator is prohibited. Users must not allow others use their district issued devices and must not use other user’s devices without authorization from IT Staff or Administration. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges and other disciplinary actions. Any user identified as a security risk may be denied access to the network.

12. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

13. Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

14. Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.

b. Students and staff engaged in producing web pages must provide system administrators with email or hard copy permissions before the web pages are published. Printed evidence of the status of "public domain" documents must be provided.

c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e. Student work may only be published if there is written permission from both the parent/guardian and student.

15. Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.

b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.

c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.

d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

e. Use of the School District's email system constitutes consent to these regulations.

16. Student Privacy - When selecting new software or websites for student educational use staff shall adhere to the following rules:

a. When implementing a new website or software that uses any type of student data, such as names, usernames, email addresses, and/or personally identifiable information of the student, a staff member shall first consult with the IT Director to determine if that website or software is on the approved software/website list. If it is not, complete the appropriate form to be granted access by the Administration. Both the list, and the form, can be found on the staff Intranet.

Violation of Policies

The failure of any user to follow the terms of the agreement will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The following consequences will be administered based on the severity of the violation.

A single consequence or any combination of the following may be administered per discretion of the School District Administrators.

1. Warning
2. Suspension from Network, technology, or computer privileges
3. General discipline steps from misconduct including detention, suspension, or expulsion from school or school related activities.
4. Legal action and/or prosecution