Ossining Union Free School District

COMPUTER NETWORK ACCEPTABLE USE POLICY FOR STUDENTS
District's Computer Network System

REGULATION

The following rules and regulations govern the use of the District's Computer Network System the District's Computer Network System and access to the Internet/e-mail:

I. Administration

- The Superintendent of Schools will designate an administrator to oversee the District's Computer Network System relative to instructional purposes.
- The administrator will monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The administrator will be responsible for disseminating and interpreting district policy and regulations governing use of the District's Computer Network at each school building level with all instructional network users.
- The administrator will coordinate staff training for proper use of the network and will ensure that staff supervising students using the District's Computer Network System provide similar training to their students. The administrator will be designated to establish a process for setting up individual and class accounts, establish a District virus protection process, and maintain the hardware in accordance with the service agreement.
- All student agreements to abide by District policy and regulations, and parental consent forms will be kept on file in the respective school building.
- The administrator is responsible for maintaining the internet filtering software and assure compliance with CIPA (Child Internet Protection Act)

II. Internet Access

- Only authorized users may use District computers and the District's Computer Network System All students must complete and return the signed Acceptable Use Policy prior to having access to the District Computer Network and the Internet/e-mail. Students will be provided access to the District's Computer Network System, the Internet and e-mail during the school day when supervised by a teacher and/or computer teaching assistant. Remote access will be provided to students at the discretion of the building administrator.
-
- Internet Access is controlled and monitored by Internet filtering software. The district reserves the right to block any sites they deem non-educational or inappropriate.
- Students (grades 1-12) will be provided with an individual logon account and password.
- Students email accounts will be created at the discretion of the building and district
- Students are not to create and post any pod casts without the authorization of a teacher.
- Students may not use any Internet sites to generate any personal non-school related personal profiles and/or profiles of any other individual, and may not access any Web pages designed by the student or other unauthorized site without the permission of a teacher, counselor, or administrator.
- Students may not construct their own personal non-school related web pages using the District's computer resources.
- Students are not allowed to download music, videos, images, and pod casts without the permission of a teacher and/or computer resource teacher/teaching assistant.
- Students will immediately inform a teacher, school employee, or system administrator if they receive access information which is inappropriate or makes them feel uncomfortable.
- Each respective classroom teacher and the computer resource teaching assistant will be required to monitor all of these activities during the use of the District's Computer Network System (including access to the Internet/e-mail).
- Access to the Ossining UFSD Guest Network is subject to the same rules and regulations identified in the District's Computer Network Acceptable Use Policy.

- The Ossining UFSD Guest Network provides access to filtered internet only.
- Access to the Guest Network is a courtesy and is meant primarily for educational purposes. Personal use of the network should not include personal music and video downloads and other activity that may have a significant impact on the quality of the wireless network.
- Access to the Ossining UFSD Ossining's Instructional Network is restricted to current students, faculty, staff, administration, and "sponsored" guests of the Ossining UFSD. Each user will be required to enter their Ossining's Instructional Network username and password before gaining access to the guest network. Out of district users may access the Ossining UFSD Guest Network with permission from a system administrator who will provide the user with a temporary username and password. Sponsored guests will need to register onto the network and have their "sponsor" approve their use via email confirmation.
- Users may gain access to the Ossining UFSD Guest Network via personal devices, in accordance with each Building Principal's rules and regulations regarding the use of personal devices.
- The district is not responsible for damage, loss, or theft of personal devices.
- District Technology Staff are not expected to support personal technologies.

III. Acceptable Use and Conduct

- Access to the District's Computer Network System (including the Internet /e-mail) is provided solely for educational purposes and research consistent with the District's mission and goals.
- Use of the District's Computer Network System (including the Internet/e-mail) is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name and access account is issued is responsible at all times for its proper use.
- All students will be issued a logon name (individual for grades 1-12, class or computer station assignment for grades Pre-K) and Individual passwords are not to be shared. Passwords may be changed periodically.
- Students will only use school approved software or view material on the Internet that is teacher approved or related to the District's curricula.
- E-mail will only be used for school and curriculum-related projects, and will not be used in violation of these or any other District policies in any respect.
- Students are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Students identifying a security problem on the District's Computer Network System must notify the appropriate teacher or administrator. Under no circumstance should the user demonstrate the problem to anyone other than to the District official or employee being notified. Students are not permitted to look for security problems, because as this may be construed as an illegal attempt to gain access.
- Students identified as a security risk or having a history of violations of District computer use guidelines may be denied access to the District's Computer Network System

IV. Prohibited Activity and Uses

The following is a list of prohibited activity concerning use of the District's Computer Network (including the Internet/e-mail). Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a student's access to the network:

- Using the network for commercial activity, including advertising or purchasing.
- Infringing on any copyrights or other intellectual property rights, including plagiarism), including copying, and/or installing receiving, transmitting or making available any copyrighted software on the District's Computer Network System.
- Downloading software on the network or any district device without permission from a teacher or system administrator.
- Using the network to receive, transmit, or make available to others obscene, offensive, harassing, discriminatory, violent, racist or sexually explicit material. For students, an exception may be made if the purpose of such access is to conduct research and both the teacher and the parent/guardian approve access.
- Posting chain letters or engaging in "spamming." (Spamming is sending annoying, unnecessary, or inappropriate messages to a large number of people.)
- Using the District's Computer Network System to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature), unless such is related to school research and is authorized by a teacher.
- If a student inadvertently accesses inappropriate information, the user should immediately notify a teacher or system administrator to protect against a claim that the user intentionally violated the Acceptable Use Policy.
- Using inappropriate language in private messages, public messages, and material posted on Web pages.
- Using another user's account or password.

- Downloading music, videos, images, or podcasts without the permission of a teacher.
- Attempting to read, delete, copy or modify the electronic (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's Computer Network System or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to creating and/or placing a computer virus on the network.
- Using the network to assist the election of any person to any office or for the promotion of or opposition to any ballot proposition, excluding student elections at Anne M. Dorner Middle School and Ossining High School.
- Generating a personal non-school related profile and/or revealing personal information about the user or any other person, including information such as their personal address, and telephone number, school location or any other such profile personal information.
- Using the network for sending or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software on the District's computers or the District's Computer Network System without the permission of the appropriate district official or employee.
- Using District computing resources for commercial or financial gain or fraud.
- Stealing data, equipment, or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, computer or phone systems, or vandalize the data of another user.
- Wastefully using finite District resources.
- Using the District's Computer Network System while access privileges are suspended or revoked.
- Using the District's Computer Network System in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

V. No Privacy Guarantee

All users of the District's Network should not expect, nor does the District guarantee privacy for electronic mail (e-mail) or any use of the District's Computer Network System. The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's Computer Network System.

VI. Sanctions

All users of the District's Network and equipment are required to comply with the District's policy and regulations governing the District's Computer Network System. Failure to comply with the policy or regulation may result in suspension of network privileges, revocation of network privileges, school suspension, Superintendent's hearing, and legal action and prosecution by the authorities.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

VII. District Responsibilities

The District makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the District assumes no responsibility for the quality, availability, accuracy, nature, or reliability of the service and/or information provided. Users of the District's Computer Network System (including Internet/e-mail) use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries or service interruptions caused by its own negligence or the errors or omissions of any user. The District also will not be responsible for unauthorized financial obligations resulting from the use of or access to the District's Computer Network System (including the Internet/e-mail).

Further, even though the District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the District policy and regulation.

VIII. Parent Notification and Responsibility

The Ossining Union Free School District will notify parents about the District Network (including the Internet/e-mail) and policies governing its use. Parents and students must sign an agreement, which will allow the student to have access to the District's Computer Network System, the Internet/e-mail. The permission form must be signed by parents/guardians and students upon the student's entry to the District Parents may request alternative activities for their child(ren) if they do not wish for their child(ren) to have access to the Internet/e-mail. Parents have the right to request the termination of their child(ren)'s individual account at any time. Notification of parents regarding the Computer Network Acceptable Use Policy for Students will be in accordance with the documents which appear as the Computer Network Acceptable Use Policy for Students (4526.1), Computer Network Acceptable Use Policy Regulation (4526.1-R), Exhibit 4526.1-E1 (Parent/Student Agreement for Use of the District Network-Secondary), Exhibit 4526.1-E2 (Parent/Student Agreement for Use of the District Network-Elementary),

The District Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting comport with the particular values of the families of the students. Although every effort will be made to monitor and protect the students, it is difficult for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. In addition to sharing the philosophy of the District, the District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District's Computer Network System (including the Internet). The District will provide students and parents with guidelines for student safety while using the Internet. Parents are responsible for monitoring their child(ren)'s use of the Internet at home and are encouraged to work closely with their child(ren) while they are using the Internet.

IX. Property Rights

The District has the right to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. Equipment purchased by the District belongs to the District and/or to BOCES, and employees, volunteers, and students in the District do not have ownership rights to any equipment loaned to them by the District. Extensive use of District equipment and software for private or personal business is strictly prohibited and will subject the violator to disciplinary action. No person will have exclusive use of District equipment unless authorized by the Superintendent.

X. Due Process

The District will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the District's Computer Network System (including the Internet). In the event there is an allegation that a student has violated the District Acceptable Use Policy, the student will be provided with a written notice of the alleged violation and an opportunity to present an explanation before a neutral administrator, or will be provided with notice and an opportunity to be heard in the manner set forth in the disciplinary code.

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the disciplinary code, the violation will be handled in accordance with the applicable provision of the disciplinary code. Employee violations of the District Acceptable Use Policy will be handled in accordance with District policy and the contractual and disciplinary provisions applicable to that employee.

XI. Academic Freedom, Selection of Material, Student Rights to Free Speech

Ossining School Board policies on Academic Freedom and Free Speech will govern the use of the Internet. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that which is relevant to the course objectives. Teachers will preview the Web sites to determine the appropriateness of the material contained in or accessed through the Web sites. Teachers will provide guidelines and lists of resources to assist their students in channelling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

XII. District Web Site

The District has established a District Web Site (www.ossiningufsd.org) and will continue to develop and update Web pages that

will provide information about the District. An administrator will be designated as responsible for coordinating and maintaining the District Web Site. School/Class Web Pages may be established to present information about the school or class activities. The administrator will coordinate with the building principals to determine the process for maintaining each school's respective Web pages. Teachers will work with the administrator to develop and maintain any special class Web pages. Students will be encouraged to contribute to the development of Web pages and update the District Web Site, but must do so under the supervision of a school administrator/teacher. Material presented on student Web pages must be related to the student's educational and District activities. The District has the right to deny the posting of information and material which is not appropriate in accordance with District policy. In addition, Extracurricular/Organization Web pages may be established. The building principal will coordinate with the administrator to establish a process and criteria for the establishment and posting of material, including links to other sites. Material presented on the Organization Web pages must relate specifically to the organization's activities. P.T.A. and Community Web pages must follow the same procedure.

XIII. Internet Safety and Education

The District provides all students with a variety of grade appropriate resources and lessons on how to safely and effectively access and navigate the internet. These resources include the use of district developed lessons as well as resources made available by Common Sense Media (www.commonsensemedia.org) Topics include but are not limited to: Cyberbullying, Online Predators, Digital Footprint, Information Fluency, and Digital Citizenship.

Adopted: November 18, 1998
Revised as a First Reading: August 22, 2007
Second Reading and Adoption: September 26, 2007
Revised First Reading: June 10, 2009
Second Reading and Adoption: July 15, 2009
Reviewed First Reading: November 1, 2011
Second Reading and Adoption: December 14, 2011
Revised First Reading: July 24, 2013
Second Reading and Adoption: August 21, 2013