UNIONDALE SCHOOL DISTRICT
Board of Education
District Technology Systems – Acceptable Use and Internet Safety Policy

A. Purpose

1. The Uniondale School District is providing employees and students with access to the District's electronic communication system, which includes Internet access.

2. The purpose of the District system is to assist in preparing students for success in life and work by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world.

3. Users may not use the District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use.

4. Users may not use the system for political lobbying, as defined by the State of New York.

5. The term "educational purpose" includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities.

B. Access to the System

1. The District Acceptable Use and Internet Safety Policy will govern all use of the District system. Student use of the system will also be governed by the disciplinary code. Employee use will also be governed by District policy.

2. The District Acceptable Use and Internet Safety Policy contains restrictions on accessing inappropriate material. However, the wide range of material available on the Internet reflects many points of view over which the district maintains no control and to which it does not necessarily subscribe.

C. Internet Safety

It is the policy of the Uniondale School District to protect students from inappropriate material on the Internet, as well to ensure the safety and security of students when using electronic communications such as electronic mail. This is done both through proper adult supervision of all students and adults using the Internet and by electronic means such as content filtering. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection

measures that block or filter Internet access and which will restrict minors' access to visual depictions that are obscene, contain child pornography, or materials harmful to minors. This filtering also will restrict adults' access to visual depictions that are obscene or contain child pornography.

Such filtering may only be removed for teachers or other adults for bona fide research or other lawful purpose with permission from the Director of Technology and/or Director of Library Media Services and Integration or his or her designee. Any use of instant messaging and chat rooms is prohibited except for educational purposes. Violations may result in cancellation privileges and disciplinary and possible legal consequences.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of minors using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of minors using district computers; and restricting minors' access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosures, use and dissemination of personal information regarding minors or other users; unauthorized online access by minors, including hacking and other unlawful activities; and access by minors to inappropriate material on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Director of Technology and/or Director of Library Media Services and Integration, as designated under the district's Computer Network or Acceptable Use Policy, shall monitor and examine all district computer network activities to ensure compliance with this policy and any accompanying regulations. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and any accompanying regulations in addition to generally accepted rules of network etiquette and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges. As part of this policy and the district's policy on acceptable use of district computers, the district shall also provide age-appropriate instruction to minors regarding appropriate online behavior, including:

- interacting with other individuals on social networking sites and in chat rooms, and

- cyberbullying awareness and response.

Instruction will be provided even if the district prohibits students from accessing social networking sites or chat rooms on district computers.

The school district is not responsible for failures in the operation or technical functioning of the Internet or its filtering or blocking system, the computers, hardware, or software used to access the Internet.

D. District Limitation of Liability

1. The District makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

E. Due Process

1. 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 system or through any District accounts.

2. In the event there is an allegation that a student has violated the District Acceptable Use Policy, the parent will be provided with an oral and/or written notice of the alleged violation and an opportunity to present an explanation. This is in accordance with the due process rights of students.

3. Employee violations of the District Acceptable Use Policy will be handled in accordance with due process rights, District policy, New York State Education Law and collective bargaining agreements.

F. Search and Seizure

1. System users shall be made aware that they have no expectation or right of privacy in the contents of their personal files on the District system since the system will be monitored by a system operator(s).

G. Copyright and Plagiarism

1. Teachers will instruct students to respect copyright laws and to request permission when appropriate.

2. Teachers will instruct students in appropriate research and citation practices.

H. District Acceptable Use and Internet Safety Policy

The following guidelines are to be applied when using the District system:

1. Threats to personal safety of students

a. Users will not post personal contact information about themselves or other people (i.e. address, telephone, school address, work address, etc.).

b. Users will not agree to meet with someone they have met on-line without their parent's or guardian's approval and participation.

c. Users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal Activities

a. Users will not commit vandalism or engage in hacking activities. Vandalism or hacking will result in cancellation of system use privileges as well as possible prosecution. Vandalism is defined as a malicious attempt to harm or destroy district equipment or materials, data or another use of the district's system or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creating or computer viruses. Tampering with or misuse of the computer system, hacking, or taking any other action inconsistent with this protocol and regulation will be viewed as a security violation. Violators will be responsible for any financial damages caused by their actions.

b. Users will not attempt to gain unauthorized access to the District system or to any other computer system beyond their authorized access.

c. Users may not possess bootleg software. Bootleg software means any software, which has been downloaded or copied, or is otherwise in the user's possession, without the appropriate registration of the software, including the payment of any fees owed to the owner of the software.

d. Users may not download or otherwise add software programs to the District system.

e. Users shall not use the District system or Internet to access, transmit or retransmit material which promotes violence or advocates destruction of property, including information concerning the manufacture of destructive devices, such as explosives, fireworks, smoke bombs, incendiary devices or the like.

f. Users shall not use the District system or Internet to access, transmit or retransmit material which advocates or promotes hatred against particular individuals or groups of individuals or advocates or promotes the superiority or inferiority of one racial, ethnic or religious group.

g. Users will not use the District system to engage in any illegal act.

3. System Security

a. Users may not utilize the network in such a way that it will disrupt the use of the network by others.

b. Staff and students are responsible for the accounts for which they have been provided passwords. Passwords should not be shared.

c. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet and/or to the District's computer system.

d. Users will immediately notify a teacher or administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.

e. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures if they download files onto the Districts' computers and/or networks. No files or disks may be loaded onto the Districts' computers and/or networks without a virus check and permission of designated district personnel.

4. Inappropriate Language

a. Restrictions against inappropriate language apply to all messages.

b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.

d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

e. Users will not harass another person. If a user is told by a person to stop sending them messages, they must stop.

f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

5. Respect for Privacy

a. Users will not repost a message that was sent to them privately without permission of the person who sent them the message.

b. Users will not post private or identifying information about any minor, other person, or themselves.

6. Respecting Resource Limits

a. Users will not download files larger than 20 megabytes without permission.

b. Users will not post chain letters or engage in "spamming".

c. Access to news groups, if granted, will be limited to acceptable discussions.

7. Inappropriate Access to Material

a. Users will not use the District system to access material that is considered profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). District employees may access the above material only in the context of legitimate research.

b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to a school administrator or other appropriate school employee. This will protect users against an allegation that they have intentionally violated the Acceptable Use and Internet Safety Policy.

8. Privileges

a. The use of the Internet and the District system by students and staff is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges and disciplinary and possible legal consequences.

I. Posting on the District system and on the Internet

1. The District's Internet Publishing Policy will inform all decisions regarding the posting of material to the District website.

2. The District reserves the right to post student work and information on the District system for the purposes of portfolio assessment, research, or other educationally relevant uses.

References:

Public Law 106-554, Children's Internet Protection Act
47 USC §254
20 USC §6777
47 CFR §§54.500 *et seq.*