Book	Administrative Procedures
Section	7000 Property
Title	STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY
Code	ap7540.03
Status	Active
Adopted	August 1, 2002
Last Revised	July 12, 2011

7540.03 - **STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY**

Students are encouraged to use the Board's computers, network, and Internet connection ("network") for educational purposes. Use of the network is a privilege, not a right. When using the network, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use of the network, including, any violation of these procedures, may result in cancellation of the privilege, disciplinary action consistent with the student handbook, and/or civil or criminal liability. All students will by default have internet access unless the AUP Opt Out Form is signed (Form 7540.03 F1). Parents are encouraged to discuss their values with their children and encourage students to make decisions regarding their use of the Internet that is in accord with their personal and family values, in addition to the Board's standards.

Smooth operation of the Board's network relies upon users adhering to the following procedures. The procedures outlined below are not exhaustive, but are provided so that users are aware of their general responsibilities.

A. Students are responsible for their behavior and communication on the network, which includes the internet!

B. Students may only access the network, Internet and any applications by using their assigned network account. Use of another person's account/address/password is prohibited. Students may not allow other users to utilize their account/address/password. Students may not go beyond their authorized access.

C. Students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the network.

D. Students may not use the network to engage in "hacking" or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography; fraud; sale of illegal substances and goods).

1. Slander and libel are terms defined specifically in law. Generally, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language. Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Students shall not knowingly or recklessly post false or defamatory information about a person or organization. Students are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.

2. Students may not use the network to harass others. Foul and abusive language, the posting of obscene images or texts, posting of information that injures another, sexual comments or images, racial slurs, gender-specific comments or any comments that would reasonably offend someone on the basis of age, sexual orientation, religious or political beliefs, national origin, disability is prohibited.

E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

F. Any use of the network for commercial purposes (e.g., purchasing or offering to sell personal products or services by students), advertising, or political lobbying is prohibited. This provision shall not limit the use of the network by students for the purpose of communicating with elected representatives or expressing views on political issues.

G. Use of the network to engage in cyber bullying is prohibited. ""Cyber bullying" is defined as the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal web sites, and defamatory online personal polling web sites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (http://www.cyberbullying.ca)]

Cyber bullying includes, but is not limited to the following:

1. posting slurs or rumors or other disparaging remarks about a student on a web site or on weblog;

2. sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;

3. using a camera phone to take and send embarrassing photographs/recordings of students;

4. posting misleading or fake photographs of students on web sites.

Note: Students are not permitted to post to any website or take or send any pictures with any device without their teacher's approval.

H. Students are expected to abide by the following generally-accepted rules of network etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the network. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive or disrespectful language in communications through the network (including, but not limited to, public messages, private messages, and material posted on web pages).

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending him/her messages, the student must stop.

4. Do not post information that, if acted upon, could cause damage or a danger of disruption.

5. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet. This prohibition includes, but is not limited to, disclosing personal identification information on commercial web sites.

6. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.

7. Never agree to get together with someone you "meet" on-line without parent approval and participation.

8. Check e-mail frequently, and diligently delete old mail on a regular basis from the personal mail directory to avoid excessive use of the electronic mail disk space.

9. Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains pornography. Students should not delete such messages until instructed to do so by a staff member.

I. Use of the network to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to the interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political or scientific value as to minors. If a student inadvertently accesses material that is prohibited by this paragraph, s/he should immediately disclose the inadvertent access to the teacher or building principal. This will protect

the user against an allegation that s/he intentionally violated this provision.

J. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited. Students may not use the network in such a way that would disrupt its use by others. Students must avoid intentionally wasting the District's computing resources. Students may not bypass or attempt to bypass the District's technology protection measure. IE: Internet/CIPA Web filter Students must immediately notify the teacher or building principal if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

K. All communications and information accessible via the Internet should be assumed to be private property (i.e. copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions/acknowledgement of authorship must be respected. Rules against plagiarism will be enforced.

L. Downloading of information onto the Board's hard drives is prohibited, without prior approval from the site manager. If a student transfers files from an internet web site or USB device, CD, DVD or any electronic media to any District Computer; the student must check the file with a virus- detection program before opening the file for use. If a student transfers a file or software program that infects the network with a virus and causes damage, the student will be liable for any and all repair costs to make the network once again fully operational.

M. Students must secure prior approval from a teacher before joining any web site, including social networking sites like facebook. Furthermore students should not post personal messages to any web site without permission from their classroom teacher.

N. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent, or building principal.

O. Privacy in communication over the Internet and the network is not guaranteed. In order to verify compliance with these procedures, the Board reserves the right to monitor, review, and inspect any directories, files and/or messages residing on or sent using the network. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

The following notice will be included as part of the computer log-on screen:

"NOTICE AND CONSENT FOR MONITORING"

"Unauthorized or improper use of this computer system and/or network is strictly prohibited. Use of any computer system, network and Internet connection must comply with the District's Computer and Internet Acceptable Use and Safety Policy. This computer system, including all related equipment, networks, and network devices (specifically including Internet access), are provided only for communication, processing, and storage of school/education-related information and/or for authorized School District use. These systems and equipment are subject to monitoring for all lawful purposes including, but not limited to, to ensure proper functioning and management of the system to protect against improper or unauthorized use or access, and to verify the presence or performance of applicable security features or procedures and operational security. Monitoring includes active attacks by authorized employees and/or agents of the School District to test or verify the security of the system. During monitoring, information may be examined, recorded, copied, and/or used for authorized purposes. All information, including personal information, placed on or sent over the system may be monitored. Such monitoring may result in the acquisition, recording, and/or analysis of all data communicated, transmitted, processed, or stored in this system by a user. Unauthorized use may subject you to disciplinary action and/or criminal prosecution. Evidence of unauthorized or improper use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this computer system, authorized or unauthorized, constitutes consent to monitoring for these purposes."

P. Use of the Internet and any information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the network will be error-free or without defect. The Board is not responsible for any damage a user may suffer, including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects should be cited the same as references to printed materials. The Board will not be responsible for financial obligations arising through the unauthorized use of the network. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of misuse of the network by the student.

Q. Disclosure, use and/or dissemination of personal identification information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian.

R. Proprietary rights in the design of web sites hosted on the Board's servers remains at all times with the Board.

S. File-sharing is strictly prohibited. Students are prohibited from downloading and/or installing file-sharing software or programs on the network. Online file sharing can cause the Districts systems to become infected with data stealing Malware, Malicious Software. It can also cause the Districts confidential data to be leaked out onto the internet!

T. Students may not establish web-based e-mail accounts on commercial services through the network (e.g., Gmail, Hotmail, Yahoo mail, etc.). Students may not access any web-based e-mail accounts not established for the student by the District/School. Any cloud computing services that require a user account must be District/School approved.

U. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the District's users will be fully investigated and disciplinary action will be taken as appropriate.

V. Preservation of Resources and Priorities of Use: Computer resources are limited. Because space on disk drives and bandwidth across the lines which connect the network (both internally and externally) are limited, neither programs nor information may be stored on the system without the permission of the site manager. Each student is permitted reasonable space to store web, and personal files. The Board reserves the right to require the purging of files in order to regain disk space. Students who require access to the network for class- or instruction-related activities have priority over other users. Students not using the network for class- related activities may be "bumped" by any student requiring access for class- or instruction-related purpose. The following hierarchy will prevail in governing access to the network:

1. Class work, assigned and supervised by a staff member.
2. Class work, specifically assigned but independently conducted.
3. Personal correspondence (e-mail – checking, composing, and sending).
4. Training (use of such programs as typing tutors, etc.).
5. Personal discovery ("surfing the Internet").
6. Other uses – access to resources for "other uses" may be further limited during the school day at the discretion of the building principal.

Non-educational game playing is not permitted at any time.

Revised 2/28/06
Revised 2/15/07
Revised 9/07
Revised 6/08
Revised 7/12/11

Legal

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended

20 U.S.C. 6301 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended

18 U.S.C. 2256

18 U.S.C. 1460

18 U.S.C. 2246