



**Official School Board Policy
of the
North Allegheny School District**

		References:		
Rev. No.	Date	School Law	Board Policy	Admin. Procedure
0	8/14/02		3640 (supersedes #2530)	3640
1	8/18/10		3640	
2	6/27/12		3640	

**COMPUTER, TELECOMMUNICATIONS AND
INFORMATION TECHNOLOGY
ACCEPTABLE USE POLICY
(STUDENTS)**

1.0 PURPOSE

This policy applies to all District students who use the District’s computers, computer networks, and Internet facilities.

For educational purposes, the use of network facilities shall include classroom activities and high-quality, educationally enriching personal research.

Internet access, email, computers, technology and network resources are available to students in the District for educational and instructional purposes and other purposes consistent with the educational mission of the District, to facilitate learning through interpersonal communications and access to information, research, and collaboration. This policy shall be available to parents and guardians of students.

2.0 SCOPE

This policy applies to all District students who use the District’s computers, laptops, mobile devices, computer networks, and Internet facilities. Parents may request that students not have individual access to District computers and Internet resources in writing.

Use of personal electronic devices by students while under District supervision is also covered by the Code of Student Conduct. In some instances, use by students of personal electronic devices may be subject to this policy.



3.0 PHILOSOPHY

- 3.1 **Advantages** – The School Board recognizes that computers, telecommunications, and information technologies, when properly used, have the ability to enhance student instruction and learning.
- 3.2 **Disadvantages** – The School Board also recognizes that the District’s powerful computers, telecommunications network, and information technologies, when improperly used, can have negative consequences, especially in the absence of proper training, responsible supervision and appropriate decision-making.
- 3.3 **Benefits Outweigh the Disadvantages** – It is the District’s position that benefits to users of the District’s computers, network, and information technologies greatly exceed the disadvantages.
- 3.4 **Privilege** – Access to and the use of the District’s computers, network and information technologies shall be considered a privilege, not a right or entitlement. This privilege may be restricted or revoked, as provided herein.
- 3.5 **Instruction in Usage** – The District shall establish procedures to ensure that students are properly instructed, on an annual basis, in appropriate online behavior in accordance with applicable state and federal law. Students shall also be educated regarding proper usage of the District’s computers, network, and information technologies.
- 3.6 **Proper Supervision** – At all levels, student computer and Internet usage will be monitored. Students shall use the Internet only under staff supervision and Principal approval and in the context of research and instruction related to the curriculum.
- 3.7 **Privacy** – Students are advised and should be aware that school files (email, files on disks, files on District computers, e.g.) are not private. The District reserves the right to log, monitor and review Internet, email, and other network use of each user on North Allegheny School District’s technology equipment. Each user of a District computer agrees and consents to such logging, monitoring and review, and acknowledges that he/she has no right or expectation of confidentiality or privacy with respect to Internet, email or other network usage.
- 3.8 **Email** – The North Allegheny School District may provide its students with email for the purpose of promoting educational excellence by facilitating



resource sharing and communication. For that reason, email should be used for only school-related purposes and not personal use. Bulk mailing should be done for academic and other expressly-approved purposes only. Unsolicited email such as chain mail, advertisements, and other such junk mail is not allowed.

3.9 Repair and Maintenance – Problems with computers, software, or any other technical equipment must be reported to a teacher or administrator. Users are responsible for keeping equipment in good repair.

3.10 File Management – Students are responsible for backing up their own work on a regular basis. The Information Technology Department advises strongly that important files are saved in multiple destinations (network, CDs, flash drives, home).

3.11 System Configuration and Security – Each school computer is configured to access the District’s network and to provide each user with the appropriate software. Changes in a computer’s configuration such as adding or deleting software, customizing desktops, and adding screen savers, can cause serious errors and failures both in a computer and the network. Do not attempt to make changes to a computer’s settings without consulting a technology staff member. Only approved hardware and software are to be used or added to the District network.

System security is protected through the use of passwords. Students shall not share their passwords.

Any security problems are to be directly and immediately reported to a teacher or other staff member. If a student discovers a security breach and demonstrates it to others or informs others about it, it shall be a violation of this policy.

4.0 STUDENT ACCESS

4.1 Behavioral Expectations – Because communications on computer networks are public in nature, and thus may be a reflection on the District, students shall be expected to be considerate and responsible and not violate the student Code of Conduct in any way while using the District’s computers, network, and information technology facilities. Students who do not comply with the behavioral expectations set forth in this policy will be subject to loss of computer privileges and disciplinary consequences under the District’s Code of Student Conduct.



4.2 Etiquette—Users are expected to abide by generally accepted rules of network etiquette. These include, but are not limited to, the following:

- 4.2.1 Do not reveal personal information about yourself or others;
- 4.2.2 Be polite and appropriate;
- 4.2.3 Use appropriate language;
- 4.2.4 Recognize that all forms of electronic information and data are not private or confidential;
- 4.2.5 Do not use the Internet or email in a way that would harm or interfere with others; and
- 4.2.6 Respect the rights of other users on the network.

4.3 If an inappropriate site is accessed containing inappropriate content such as, but not limited to online violence, pornography, bigotry, gambling or illegal activities, a student is expected to notify his or her teacher immediately.

4.4 Students will be expected to participate in training programs which will address topics such as (a) how to handle appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and (b) how to increase awareness for the prevention of cyber bullying and the appropriate responses to cyber bullying. Bullying in any form will not be tolerated in the North Allegheny School District.

4.5 Students will be encouraged to report bullying or cyber bullying complaints to District employees. Such complaints can be made orally and/or in writing to any District employee.

5.0 BLOCKING OF INAPPROPRIATE WEBSITES

5.1 Blocking Devices: The District shall implement filtering technology to ensure that students are protected from inappropriate content on the Internet in accordance with the Child Internet Protection Act (CIPA). The District currently uses an appropriate program or filter to protect against access to visual depictions that are obscene, pornographic, or harmful to minors, as defined by CIPA. At the discretion of the District, the network may be configured to protect against access to other material considered inappropriate



for users to access. The program or filter used for protection will be configured and updated by the District in a reasonable fashion, and may be replaced by the District with an equivalent program at the District's discretion.

5.2 Request that a Website be Unblocked: If a student user believes that a website that is blocked should be available to all users, that student shall request that the block from that particular website be removed. The student shall request through a staff member that a site be unblocked. Thereafter, the District shall follow the established protocol for reviewing the site in question to determine whether it should be unblocked. If it is determined that the website should be unblocked, the network administrators shall be directed to unblock the website within ten (10) days of that determination.

5.3 Disabling the Blocking Software: The blocking software shall not be intentionally disabled at any time that students may be using the District's computers and Internet resources, if such disabling would cease to protect against access to materials that are prohibited under CIPA.

6.0 IMPROPER USAGE

6.1 Students who intentionally use the District's computers, network, and information technology facilities in any manner such as those prohibited in Section 6, 7, and 8 of this policy may be denied future access, and usage shall be subject to a loss of computer and Internet privileges, disciplinary action in accordance with the rules and regulations of the Code of Student Conduct and, where applicable, appropriate federal, state, and local statutes, ordinances, and regulations. When it is deemed necessary, law enforcement will be contacted.

6.2 The following are considered to be examples, but not an all-inclusive list, of improper usage that violate this policy and which may constitute violations of the Code of Student Conduct.

6.2.1 Attempting to invade or damage facilities, equipment, software, or supplies.

6.2.2 Sending e-mail for personal and non-approved use by students.

6.2.3 Using, sending, displaying or disseminating offensive, abusive, or obscene language, files, photographs, images or material through the District's computer and network systems.



- 6.2.4 Harassing, insulting, or attacking others by use of the District's computer and network systems.
- 6.2.5 Visiting chat rooms in a non-educational or unapproved context.
- 6.2.6 Obtaining pornographic or sexually-explicit materials by use of the District's computer and network systems.
- 6.2.7 Building, maintaining, or supporting personal, non-academic websites on the District's network.
- 6.2.8 Violating copyright laws and/or licensing agreements by use of the District's computer and network systems.
- 6.2.9 Using another's password or account.
- 6.2.10 Sharing passwords.
- 6.2.11 Attempting to violate or circumvent security procedures.
- 6.2.12 Trespassing, transferring, reading, changing, modifying, copying, sharing, or destroying another's files.
- 6.2.13 Intentionally wasting resources, such as disc space, bandwidth, or printing capacity. For example, using network resources to save large non-educational files or for the streaming of video and music on such sites as YouTube and Pandora may significantly degrade network performance.
- 6.2.14 Employing the District's computer or network systems for unapproved commercial or political purposes.
- 6.2.15 Using facilities, software, or supplies for any purposes not directly related to school activities.
- 6.2.16 Downloading, installing, or using unauthorized software, including but not limited to shareware, freeware, games, and audio/video files. Authorization to install any software on District computers shall come from only the Information Technology Department.
- 6.2.17 Attempting to make unauthorized purchases on the Internet that result in an expense to the District.



- 6.2.18 Using facilities in any way deemed by the District, in its sole discretion, to be inappropriate.
- 6.2.19 Violating any federal, state, or local statutes, ordinances, or regulations relative to computer, software, network, and Internet usage.
- 6.2.20 Writing, producing, or generating any computer code or message on the network that might disrupt or adversely affect any network user or resources.
- 6.2.21 Hacking, cracking, or otherwise trying to gain access to the District network or another person's or organization's computer system.
- 6.2.22 Giving another person's personal information such as name, address, phone number, or gender out in an electronic communication such as an email.
- 6.2.23 Using Google Apps for Education for non-school-related work.

7.0 SOCIAL MEDIA/SOCIAL NETWORKING ETIQUETTE

These guidelines apply to students who, as part of District-approved educational activities, choose to and are permitted to create or contribute to blogs, wikis, social networks, virtual worlds, or any other kinds of social media. All of these tools can be beneficial to enhance the educational experience. The District expects that anyone who participates in online communities or networking to understand and follow these simple but important rules of engagement.

- 7.1** The overall goal is simple: demonstrate integrity. Every student of the North Allegheny School District who participates online shall do so in a respectful, relevant way that supports the mission and vision of the District, and protects the reputation of the District in every regard: the following are intended to provide specific guidelines for online participation.
 - 7.1.1 Post meaningful, respectful comments.
 - 7.1.2 Use common sense and common courtesy. Be aware that everything you write is public.
 - 7.1.3 Never violate another person's privacy or confidentiality online.



- 7.1.4 You are responsible for ensuring that anything posted or downloaded does not violate applicable copyright law. This is a consideration when selecting music, images, text, etc., to include in any posting or when copying, downloading or using music, images, text, graphics, sound or video clips or software.
- 7.1.5 Carefully review the content of any links before embedding them as a part of your commentary to ensure that it meets the standards set by the District for student review.
- 7.1.6 When disagreeing with the opinions of others, be appropriate and polite.
- 7.1.7 If you are repeating something someone else has said, make certain you have their permission first.
- 7.1.8 If you are naming another individual, especially a student, in your commentary, do not provide any identifying information about the individual. Use a non-specific identifier, such as a first initial or pseudonym. No one may use the District's network to publish or otherwise use a student's personally identifiable educational records without permission of the student (if over age 18), or the student's parents.
- 7.1.9 Remember that even anonymous comments you post may be traced back to you or the District's IP address, and you will be held responsible for them.
- 7.1.10 Be smart and thoughtful about protecting yourself, your privacy and the District's confidential information. What you publish is widely accessible and will be around for a long time.
- 7.1.11 By posting content online, you warrant that you own or otherwise control all of the necessary rights to that content. Plagiarism is prohibited.
- 7.1.12 The District does not pre-screen any content that is posted on the Internet, but it shall have the right to remove, in its discretion, any content that it considers to violate the terms of this Acceptable Use Policy or the Code of Student Conduct.
- 7.1.13 The District's computer and Internet facilities shall not be used to engage in hate mail, harassment, discriminatory remarks, offensive, inflammatory, threatening statements and other antisocial communications on the network. Users shall not engage in personal attacks, including prejudicial



or discriminatory attacks. Users shall not harass another person. Harassment is defined as persistently acting in a manner that distresses or annoys another person. If users are told by a person to stop sending them messages, they must stop. Users shall not knowingly or recklessly post false or defamatory information about a person or organization.

7.1.14 You must not post material that is knowingly false, misleading, or inaccurate.

7.1.15 You must not impersonate any person or entity, or forge or manipulate identifiers in order to disguise the origin of any posting.

7.1.16 Any access to sites not consistent with North Allegheny's educational and community service goals is prohibited.

7.1.17 No one may use the North Allegheny network to access or distribute material that (1) is obscene or indecent, (2) is patently offensive as measured by contemporary community standards, (3) is sexually explicit, (4) tends to degrade any race, religion, ethnic origin, or gender.

8.0 DISCLAIMER – The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District will not guarantee that the functions or services provided through the District's Internet service will be without error. The District is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non deliveries, missed deliveries, or service interruption, caused by its own negligence or the user's errors or omissions, any hardware failure, or exposure to inappropriate material or people. Use of any information obtained through the use of the District's computers is at the user's risk. The District disclaims responsibility for the accuracy or quality of information obtained through the Internet or e-mail. A student's parents or guardians can be held financially responsible for any harm that may result to the District's computer and network systems from the student's intentional misuse of the system. Each school shall provide an annual written notice to the parents or guardians of students about the District's Internet system, the policies governing its use, and the limitation of liability of the District. Parents and guardians shall sign a document indicating their receipt of the annual written notice concerning the District's Acceptable Use Policy. Upon receipt of the executed notice, the student will be permitted to access the District's network/Internet resources. Parents and guardians have the right to request the termination of their child's network/Internet access at any time.