3.0 PHILOSOPHY

3.1 Advantages – The School Board recognizes that computers and telecommunication/information technologies, when properly used, have the ability to enhance student learning and staff and administrative functions.

3.2 Disadvantages – The School Board also recognizes that the District's computers and telecommunication/information technologies, when improperly used, can have negative consequences, especially in the absence of responsible supervision and appropriate decision-making.

3.3 Benefits Outweigh the Disadvantages – It is the District's position that the benefits to the users of the District's computers, network and information technologies greatly exceed the potential disadvantages of said technologies.

3.4 Privilege – Access to and the use of the District's computers, network and information technologies shall be considered a staff member's privilege, and not a right or entitlement.

3.5 Instruction in Usage – The District shall establish procedures and ensure that staff are properly instructed in the appropriate usage of the District's computers, network and information technologies.

3.6 Filtering Program – The District shall employ a firewall and a filtering program that monitors and blocks objectionable materials from being accessed or received over the Internet.

3.7 Privacy – Please be advised that school files (email, files on disks, files on your computer, 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 Districts technology equipment. Each user of a District computer agrees and consents to such logging, monitoring and review and acknowledges that he or she has no right or expectation of confidentiality or privacy with respect to Internet, email or other network usage. Employees should never share their password with anyone other than authorized network technicians.

3.8 Email – The North Allegheny School District provides its staff with email for the purpose of promoting educational excellence by facilitating resource sharing and communication. For that reason, email should be used for school-related purposes only. Bulk or mass emailing should be done for work-related purposes only. Unsolicited email such as chain mail, advertisements or other such junk mail is not allowed. Email passwords should be kept confidential.

3.9 **Repair and Maintenance** – Problems with computers, software or any other technical equipment must be communicated by email or phone to the Help Desk.

3.10 **File Management** – Faculty and staff members are responsible for backing up their own work on a regular basis. The Information Technology Department advises strongly that you save your important files in multiple destinations (network, USB devices, 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 user's computer and the network. Staff members must not attempt to make changes to a District computer's settings without consulting a technology staff member. Only approved hardware is to be used or added to the District network. System security is protected through the use of passwords. Failing to adequately protect one's password could result in unauthorized access of personal information or school files such as grades, discipline, etc.

Any security problems are to be directly reported to the Information Technology Department and are not to be demonstrated to others.

4.0 ACCESS TO AND USE OF FACILITIES

4.1 **Employees** – The District's computers, network and information technologies may be made readily available to staff members and considered as tools that are integral to the discharge of their respective duties. To limit the liability of the District, the policy will be distributed electronically to all staff members for their review and will then be permanently posted to the District website. Staff members will be asked to sign or otherwise indicate receipt of this Policy. Long term substitute employees will also be permitted access.

4.2 **Volunteers** – Volunteers and other non-employees may have access to and be permitted to use the District's computers, network and technology facilities only when prior written permission is granted by a professional or administrative employee and only while their access and usage is properly monitored and supervised by the employee who granted permission. Such requests are to be filed in the building office of the staff member making this request.

4.3 **Training** – To ensure the proper and efficient usage of the District's computers, network, and information technology facilities, appropriate training programs shall be established and maintained for staff members.

4.4 **Behavioral Expectations** – Because communications on computer networks are public in nature, and thus may be a reflection on the District, staff members shall be expected to be considerate and responsible while using the District's computers, network and information technology facilities and follow the guidelines set forth in this Policy.

4.5 **Access to Staff/Volunteer Data** – All staff or volunteer-generated data, files and communications may be reviewed by network administrators to ensure that network system integrity is maintained and that the network system is being used in a responsible manner. Information stored on District servers shall not be private, and employees shall have no expectation of privacy.

4.6 **Etiquette** – Staff users are expected to abide by the generally accepted rules of network etiquette in using the District's computer and network resources. These include but are not limited to the following:

- Be polite and appropriate.
- Use appropriate language.
- It is recommended that staff members not reveal personal information (address, telephone number) of self or others.
- Recognize that all form of electronic information and data is not private or confidential.
- Do not use the Internet or email in a way that would harass or interfere with others.
- Respect the rights of other users on the network.

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 or staff user believes that a website that is blocked should be available to all users, that student or staff member shall request that the block from that particular website be removed. The staff member shall relay a student's request 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.

5.4 **Child Internet Protection Act (CIPA) Training** – All appropriate staff in the District shall participate in educating students on how to handle appropriate online behavior, including interacting with other individuals on social networking websites and chat rooms and increasing cyber bullying awareness and the appropriate responses to such activity. Specifically with regard to cyber bullying, the following protocols shall be followed by staff members:

- Any staff members who receive a bullying complaint from a student shall immediately notify the building principal.
- The building principal will investigate the alleged conduct that occurred.
- If the behavior is found to meet the definition of bullying, the building principal will follow through with corrective action to ensure that the behavior ceases. If necessary or warranted, the offending student may be subject to disciplinary action as outlined in the Code of Student Conduct.

6.0 IMPROPER USAGE

Staff members shall not engage in improper uses or conduct regarding the District's computer and network resources and telecommunication/information technologies. The following are considered to be examples, but not an all-inclusive list of types of improper usage and conduct:

6.1 Use of resources or technologies to infiltrate or interfere with a computer system and/or damage the data, files, operations, and software or hardware components of a computer or system.

6.2 Stealing computer equipment, software, or supplies.

6.3 Intentionally sending or displaying offensive messages or images.

6.4 Using offensive, abusive, or obscene language in connection with use of computer and network resources and telecommunication/information technologies.

6.5 Using computer and network resources or telecommunications/information technologies to make harassing or insulting remarks or attacking others, including hate mail, discriminatory remarks, threatening statements or other antisocial communications.

6.6 Violating copyright laws and/or licensing agreements.

6.7 Using another's password or account without prior approval from the user and/or the Information Technology Department.

6.8 Sharing passwords with students or other unauthorized individuals.

6.9 Attempting to violate or circumvent security procedures.

6.10 Trespassing in another's folders or files.

6.11 Transferring, reading, changing, modifying, copying, sharing, or destroying another user's data, information, or passwords.

6.12 Intentionally wasting computer, network or technology resources, such as disk space, bandwidth, or printing capacity.

6.13 Employing the District's computer network for commercial, for- profit or political purposes.

6.14 Using facilities, software, or supplies for any purposes not directly related to school activities.

6.15 Installing or using unauthorized software, including, but not limited to, shareware, freeware or games, programs, files, music, or other electronic media. Authorization to install any software on District computers or telecommunications/information technologies must come from the Information Technology Department.

6.16 Attempting to make unauthorized purchases on the Internet which result in an expense to the District.

6.17 Violating any federal, state, or local statutes, ordinances, or regulations relative to computer, software, network, and Internet usage.

6.18 Writing, producing, or generating any computer code or message on the network that might disrupt or adversely affect any network user or resources.

6.19 Hacking, cracking, or otherwise trying to gain access to the District network or another person's or organization's computer system.

6.20 Use of computer network or information technology resources to access, view or obtain material that is pornographic in nature.

6.21 The unauthorized disclosure, use or dissemination of personal information regarding minors.

6.22 Any other uses deemed inappropriate by North Allegheny School District.

7.0 SOCIAL MEDIA/SOCIAL NETWORKING ETIQUETTE

The following guidelines shall apply to staff members who choose 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 of students. The District expects anyone who participates in online commentary to understand and follow these simple, but important rules of engagement.

Staff members who participate in social networking should do so only in work-related and instructionally-related ways during school hours. Staff members who participate in social networking during non-work hours should be sensitive to the fact that they are viewed by the public as role models in their capacity as public servants and should take care to ensure that their communications are appropriate and would not reflect poorly on the staff member or the District if viewed by members of the community or students.

The overall goal is simple: demonstrate integrity. Every employee of the North Allegheny School District who chooses or is obligated to participate in activities conducted online must do so in a respectful, relevant way that supports the mission and vision of the District, follows the letter and spirit of the law, and protects the reputation of the District in every regard. The following are intended as guidelines and expectations:

7.1 Always be transparent and state that you work for the North Allegheny School District. Use your real name and be clear about your role.

7.2 Never represent yourself or the District in a false or misleading way. All statements made should be true and not misleading; all claims must be substantiated.

7.3 Post meaningful, respectful comments.

7.4 Use common sense and common courtesy. Be aware that everything you write is public.

7.5 Never violate privacy, confidentiality or legal guidelines online. It is important to keep in mind that FERPA and other state and federal statutes and regulations apply to all online instructions.

7.6 Obey all copyright laws. This is a consideration when selecting music, images, text, graphics, videos and sound clips, etc., to include in any posting or project.

7.7 Carefully review the content of any links before embedding them as a part of your commentary to ensure that such links meet the standards set by the District for student review.

7.8 Stick to your area of expertise and responsibility. Feel free to provide unique, individual perspectives on non-confidential topics within your realm of authority as they pertain to the furtherance of your job objectives.

7.9 When disagreeing with the opinions of others, be appropriate and polite.

7.10 If you are repeating something someone else has said, make certain you have their permission first.

7.11 If you are naming another individual, especially a student, in your commentary, use a non-specific identifier, such as a first initial or pseudonym. Do not provide any identifying information about any individual online.

7.12 Never comment on anything related to legal matters, litigation, politics, religion, for-profit businesses, personnel matters, a crisis situation, current or past, or other such topics.

7.13 Remember that even anonymous comments you post can be traced back to you or the District's IP address.

7.14 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.

7.15 All electronic communications between staff members and students should be appropriate and solely related to academic or instructional content or issues.

7.16 A staff member may not use the North Allegheny School District name to endorse or promote any product or commercial use, non-educational cause or political candidate.

7.17 By posting content online, the staff member warrants that he/she either owns or otherwise controls all of the rights to that content.

7.18 The employee acknowledges that the District does not pre-screen any content that is posted on the Internet, but it shall have the right to remove at its discretion any content that it considers to violate the terms of this Acceptable Use Policy.

7.19 Any electronic communications that discriminate against staff members or community members by virtue of race, gender, nationality, religion or other protected classification will be dealt with according to the District policy.

7.20 Staff members must recognize that the staff member is legally liable for anything that he or she writes or presents online.

7.21 Staff members must not post material that is knowingly false, misleading, or inaccurate.

7.22 Do not impersonate any person or entity, forge or manipulate identifiers in order to disguise the origin of any posting.

7.23 Any access to sites not consistent with the District's educational and community service goals is prohibited.

7.24 No one may use the District's 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, or (4) tends to degrade any race, religion, ethnic origin, or gender.

7.25 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.

8.0 SOFTWARE POLICIES

8.1 **Policy and Procedures** – North Allegheny School District employees and staff members must respect all computer software copyrights and adhere to the terms of use for all software licenses to which the District is a party. Staff members may not duplicate any licensed software or related documentation for use either on school premises or elsewhere unless authorized by the District. Unauthorized duplication of software may subject employees and/or the District to both civil and criminal penalties under the United States Copyright Act. Staff members may not give stand alone software to any other employee.

8.2 **Acquisition of Software** – To purchase software, staff members must obtain approval from their building principal and the Information Technology Department. An employee using private funds may not purchase software. The

District maintains a complete record of all software purchases for the purpose of software registration, support, tracking, and necessary upgrades.

8.3 **Software Registration** – The District's Information Technology Department will be responsible for registering all software. Software must be registered in the name of the District. Because of personnel turnover, software should never be registered in the name of the individual user.

8.4 **Installation of Software** – No software shall be installed on District computers without the approval of the building principal and Information Technology Department. At no time shall a student install computer software. It is the responsibility of teachers and other faculty members to monitor student use of computers.

8.5 **Software Audits** – The Information Technology Department will conduct random audits of all District computers to ensure that the District is in compliance with all software licenses.

9.0 CONSEQUENCES FOR IMPROPER USAGE

9.1 **Employees** – Employees, staff members, volunteers, and any other non-students who intentionally use the District's computers, network, and Information Technology facilities in any manner such as delineated in the preceding paragraph may be denied future access and usage. Employees shall be subject to disciplinary action in accordance with the rules and regulations of the North Allegheny School District Employee Handbook/Administrative Procedure Manual and/or appropriate federal, state, and local statutes, ordinances, and regulations. When it is deemed necessary, law enforcement will be contacted.

10. DISCLAIMER – The District makes no warranties of any kind, whether express or implied, for the service it is providing through its network and computer resources. The District will not guarantee that the functions or services provided through the District's Internet and computer network 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, missed deliveries or service interruption caused by its own negligence or equipment, hardware or technology failure or the user's errors or omissions.