NORTH ALLEGHENY SCHOOL DISTRICT

SECTION:	**ADMINISTRATIVE EMPLOYEES**
TITLE:	**RESPONSIBLE COMPUTER, TELECOMMUNICATIONS, AND INFORMATION TECHNOLOGY USE**
ADOPTED:	**7/20/16**
REVISED:	

352 - RESPONSIBLE COMPUTER, TELECOMMUNICATIONS, AND INFORMATION TECHNOLOGY USE

Section 1. Purpose

a. The North Allegheny School District provides employees access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, internet access, mobile devices, peripherals, copiers, and cameras.

b. The Board supports the use of the District's technology resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the educational mission of the District, and to carry out the legitimate business and operation of the District.

c. The use of the District's technology resources is for appropriate school-related educational and operational purposes consistent with the educational mission of the District. Use for educational purposes is defined as use that is consistent with the curriculum adopted by the District as well as the varied professional responsibilities of employees. All use for any purpose must comply with this policy and all other applicable policies, procedures, and rules and must not cause damage to the District's technology resources.

Section 2. Definitions

a. Privilege - access to and the use of the District's computers, network and information technologies shall be considered a privilege, and not a right or entitlement.

b. Instruction in Usage - the District shall establish procedures and ensure that employees are properly instructed in the appropriate usage of the District's computers, network and information technologies.

c. Filtering Program - a firewall and/or a filtering program that monitors and blocks objectionable materials from being accessed or received over the

	Internet. d. System Configuration - each school computer is configured to access the District's network and to provide each user with the appropriate software. e. District Technology Resources - all technology owned and/or operated by the District, including computers, projectors, televisions, video, and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, routers, and networks, including the Internet. f. User - Anyone who utilizes or attempts to utilize District technology resources while on or off District property. The term includes, but is not limited to, students, employees, parent(s) and/or guardian(s), and any visitors to the District that may use District technology. **Section 3. <u>Access To And Use of Facilities</u>** a. The District's computers, network, and information technologies may be made readily available to administrative employees and considered as tools that are integral to their professional responsibilities and obligations. District technology resources may be assigned or allocated to an individual user for his or her use (e.g., individual e-mail accounts, laptop computers, etc.). Despite being allocated to a particular user, the technology resources remain the property of the District and may be revoked, suspended, or inspected at any time to ensure compliance with this and other District policies. Any security problems are to be reported to the Information Technology Department and are not to be demonstrated to others.
24 P.S. Sec. 4604	b. This policy will be distributed to all employees for their review and will be permanently posted to the District's website. Employees will be asked to sign or otherwise indicate receipt of this policy. **Section 4. <u>Internet Filtering and CIPA Compliance</u>**
47 U.S.C. Sec. 254 47 CFR Sec. 54.520	a. The District utilizes content and message filters to prevent users from accessing material through District technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the District's educational mission. The filtering software shall not be intentionally disabled at any time; such acts may result in disciplinary action.
24 P.S. Sec. 4601, 4604, 4610 20 U.S.C. Sec. 6777	b. The Superintendent or designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the District's filters for a bona fide educational purpose.

Section 5. Guidelines

a. The District reserves the right to monitor any user's utilization of District technology resources. Users have no expectation of privacy while using District technology resources whether on or off District property. The District may monitor, inspect, copy, and review any and all usage of District technology resources including information transmitted and received via the Internet to ensure compliance with this and other District policies, and state and federal law. All e-mails and messages, as well as any files stored on District technology resources may be inspected at any time for any reason.

b. District technology resources shall be periodically monitored to ensure compliance with this and other District policies including monitoring of users' online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. Violations of this policy or any other School District policy, may be discovered by routine maintenance and monitoring of the District technology environment. However, the Superintendent, or his/her designee, shall also implement procedures to ensure that District technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated cameras and/or audio are not utilized.

17 U.S.C.
Sec. 101 et seq.
Pol. 814

c. Federal laws, cases, and guidelines pertaining to copyright govern the use of material accessed through District resources. Users will make a standard practice of requesting permission from the holder of the work; comply with the Fair Use Doctrine, and/or complying with license agreements. Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over networks, remixing or preparing mash-ups, and deep-linking into the content of others' web sites.

d. Users may not circumvent technology protection measures that control access to a protected work unless they are permitted to do so by law.

e. Employees shall not engage in improper uses or conduct regarding the District's technology resources. The following are considered to be examples, but not an all-inclusive list of types of improper usage and conduct:

1. Stealing or intentionally harming computer equipment, software, or supplies and/or intentionally wasting computer, network or technology resources, such as bandwidth, or printing capacity.

2. Installing or using unauthorized software, including, but not limited to, shareware, freeware or games, programs, files, music, or other electronic media.

	3. Attempting to violate or circumvent security procedures by trying to gain access to the District network or another computer system or infiltrating or interfering with a computer system
	4. Using technology resources to bully or to create, access, or to distribute harassing, obscene, lewd, vulgar, or pornographic remarks, insulting remarks, or attacking others, including hate mail, threatening statements or other antisocial communications.
Pol. 248, 249	5. Accessing, viewing, displaying, creating, or sending material that is offensive, abusive, obscene, and/or pornographic in nature or tends to degrade any race, religion, ethnic origin, or gender.
SC 1317.1 18 Pa C.S.A. Sec. 5903	6. Using technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.
	7. Sharing or using another's password(s), account(s), or credentials for electronic accesses to resources and equipment.
	8. Accessing another user's files without explicit permission.
	9. Employing technology resources for commercial, for-profit, or any purposes not directly related to school activities or business.
	10. Using technology resources to gamble.
	11. Using technology resources for political lobbying or campaigning, not including student elections (e.g., student government, club officers, homecoming queen, etc.).
	12. Connecting or tethering a non-District owned device to access an unfiltered and/or unmonitored internet connection.
	13. Using proxies or other means to bypass internet content filters and monitoring.
	14. Concealing, or attempting to conceal, a user's identity, including the use of anonymizers, or the impersonation of another user.
	15. Accessing restricted system settings or changing settings or access rights to a restricted system or account.
	16. Use of encryption software that has not been previously approved by the District.
	17. Scanning the District's technology resources for security vulnerabilities.
	18. Attempting to make unauthorized purchases on the Internet which result

in an expense to the District.

19. Disclosing or disseminating personal information regarding minors.

20. Use of the "North Allegheny School District" or its logo for non-District activities, endorsement of products, or any 'for profit' activities without the express written permission of the Superintendent or designee.

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

Section 6. Consequences for Improper Usage

24 P.S.
Sec. 4604

Violations of this policy may result in the temporary or permanent loss of computer and Internet privileges or disciplinary action in accordance with the Act 93 Agreement and/or federal, state, and local laws.

Section 7. Disclaimer

The District makes no warranties, 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.

References:
School Code – 24 P.S. Sec. 510, 1317
PA Crimes Code – 18 Pa. C.S.A., Sec. 5903
Child Internet Protection Act – 24 P.S. Sec. 4601, 4604, 4610 et seq.
Internet Safety, Children's Internet Protection Act – 47 U.S.C., Sec. 254
U.S. Copyright Law – 17 U.S.C., Sec. 101 et seq.
Enhancing Education Through Technology Act – 20 U.S.C., Sec. 6777
Children's Internet Protection Act – Certifications, Title 47, Code of Federal Regulations – 47 CFR, Sec. 54.520
Pol. 248, 249, 708, 814

Replaces Policy:
5610