Adoption Date:	09/15/2014
Revision Date(s):	

Arts Academy Charter School
1610 East Emmaus Avenue
Allentown, PA 18103
arts-cs.org

Board Policy 9.1.2

Acceptable Use of the Internet and School Network

Section 1. Purpose

The Arts Academy Charter School (herein referred to as AACS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop skills in technology and technology-based communication. To that end, AACS provides a network that enables students and staff to access the internet as well as access to computers and other devices. While AACS believes that the knowledge and skills derived from and about the internet are invaluable, it also recognizes some of the inherent dangers that the internet poses. AACS is committed to ensuring internet safety to the greatest extent possible. This Policy governs the appropriate use of AACS's network and the internet, as set forth, below.

Section 2. Definitions

Child Pornography - Under federal law, this term means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Under Pennsylvania law, the term means any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

For the purposes of this Policy, Child Pornography includes material/content that meets either the Pennsylvania or the federal standard or both.

Harmful to Minors - Under federal law, this term means any picture, image, graphic image file or other visual depictions that:

1. Is taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion.

2. 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 content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals.

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors.

Under Pennsylvania law, this term means any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors.

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors.

3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.

For the purposes of this Policy, "harmful to minors" includes material/content that meets either the Pennsylvania or the federal standard or both.

Incidental Personal Use – This term refers to use of the internet and school's network by AACS employees that does not interfere with the employee's job duties and performance, with system operations, or with other system users. Incidental personal use must comply with this policy, accompanying administrative regulations, and all other applicable school policies, regulations, procedures and rules, as well as ISP terms, local, state and federal laws. Incidental personal use must not damage or cause harm to school technology or the school's network.

Minor – This term, for purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen (17). For other purposes, "minor" shall mean the age of minority as defined in the relevant law.

Network – The term "network," for the purposes of this Policy, includes AACS's server(s) and any and all access to the information stored thereon, whether retrieved through a wired device or wireless access, including the use and/or access to the internet or other servers or networks through AACS's server. The term also expressly includes any system linking two (2) or more school electronic devices.

Obscene - under federal law, analysis of the material meets the following elements:

1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene.

3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

Under Pennsylvania law, analysis of the material meets the following elements:

1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene.

3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.

For the purposes of this Policy, "obscene" includes material/content that meets either the Pennsylvania or the federal standard or both. For the purposes of this Policy, "obscene" shall also include any and all gratuitous nudity or partial nudity without social or artistic value or nude/partially nude images that are being accessed for prurient purposes, regardless of the image's intrinsic social or artistic value. This definition shall expressly include all forms of sexting and the sending, viewing or possession of nude or partially nude photographs via cell phone, email, internet, social media, or other electronic form.

Sexual Act and Sexual Contact – This term shall be interpreted consistent with 18 U.S.C. Sec. 2246, and at 18 Pa. C.S.A. Sec. 5903.

Social Media – The term "social media," for the purposes of this Policy, includes all web-based services that allow individuals to (1) construct a public, semi-public or private profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections made by others within the system. Such sites include Facebook and MySpace. The term shall also expressly include all other interactive websites, such as blog sites and microblogs (such as Twitter), virtual worlds (such as World of Warcraft,

Second Life), video/audio/photo sharing sites (such as Instagram, Pinterest, YouTube, Flickr, photo upload sites, etc.), instant messaging, podcasts, chatrooms and other interactive online forums. This term shall also expressly include all non-AACS email accounts and sites. This term expressly excludes collaborative websites that are contained within AACS's web domain (www. www.arts-cs.org) or AACS -sponsored collaboration sites for which the building or AACS administration has approved and has provided assurance, in writing, that the site does not permit collaboration by members of the public outside of the school, meets the safety and quality standards and requirements set forth in this Policy. In addition, with any collaborative website and/or service where private communication can occur, all communications may be recorded, and can only be accessed/used by AACS faculty, staff, and student body.

Technology Protection Measure(s) – This includes, but is not limited to, the use of a specific technology or specific technologies that block(s) or filter(s) internet access to visual depictions that are obscene, child pornography or harmful to minors. 47 U.S.C. § 254(h)(7)(I); 24 P.S. § 4606.

Visual Depictions – This term includes undeveloped film and videotape, and data stored on a computer disk or by electronic means which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words. 18 U.S.C. § 1460 (b); 18 Pa.C.S.A. § 2256.

Section 3. Delegation of Responsibility

The Executive Director is granted the authority to create an administrative regulation to accompany this policy. The Executive Director is also granted the authority to create an administrative regulation that specifically addresses teacher-student communication when social networking tools are used. It shall be the responsibility of each building administrator to ensure that this Policy is followed appropriately in his/her building and to determine what is an acceptable use of the internet under this Policy and any accompanying administrative regulations. It is the responsibility of the IT/IS Manager to ensure that the network is properly maintained in accordance with the guidelines set forth in this Policy.

Section 4. Guidelines and Requirements

Acknowledgement and Consent

A copy of this policy and *CIS Acknowledgement and Consent Form* will be provided to all users, who must sign the school's *CIS Acknowledgement and Consent Form*. Users must be capable and able to use the school's CIS systems and software relevant to the employee's responsibilities.

Adoption Date:	09/15/2014
Revision Date(s):	

Access and Restriction of Access
Access to the School's network is a privilege, not a right. The school reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The school will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604.

The school reserves the right to restrict or limit usage of lower priority CIS systems and computer uses when network and computing requirements exceed available capacity according to the following priorities:

1. Highest - uses that directly support the education of the students;

2. Medium - uses that indirectly benefit the education of the student;

3. Lowest - uses that include reasonable and limited educationally-related employee interpersonal communications and employee limited incidental personal use; and,

4. Forbidden - all activities in violation of this policy, its accompanying administrative regulation, other school policies, regulations, rules, procedures, ISP terms, and local, state or federal law.

The school additionally reserves the right to:

1. Determine which network services and/or AACS technology will be provided through school resources;

2. Determine the types of files that may be stored on school file servers and computers;

3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through AACS's network and electronic communications systems and/or on AACS technology, including e-mail, text messages, and other electronic communications;

4. Remove from the network, AACS servers or school-owned devices excess e-mail and other electronic communications or files taking up an inordinate amount of fileserver space after a reasonable time; and,

5. Revoke User privileges, remove user accounts, or refer to legal authorities, and or school authorities when violation of this and any other applicable school policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, and destruction of School resources and equipment.

6. AACS reserves the right to remove all school-related Microsoft Exchange Accounts and related data from personal devices at any time as explained in the agreement presented to the user as each device has the account added.

Internet/Network Use Restricted to Educational Purposes
Use of AACS's network and the internet is limited exclusively to use for educational purposes. Personal and/or recreational use of the internet shall not be permitted on AACS's network.

Non-Network Access Prohibited
All access to the internet by students while on school grounds or at school-sponsored functions/trips must be through AACS's network. Access to the internet during school hours via 3G/4G-capable devices or other non-AACS connections, including personal WiFi hotspots, is expressly prohibited. Employees are prohibited from accessing the internet from a non-AACS connection during the school day. Employees who wish to access the internet via 3G/4G devices or other non-AACS connections outside of the regular school day but while acting in the scope of their employment must obtain specific **written** permission from the building principal.

Internet Access / Restrictions on AACS Network
AACS provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

AACS will maintain a usage log and will monitor the online activities of minors using AACS's network.

Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it should not be, the user should follow protocol to alert an IT staff member or submit a work order. If a site is accessible that contains content that is permissible under this or another Board Policy, the user is required to immediately report it to the building principal.

Because of the nature of the filter and blocking technology, as well as the technology that allows the internet to operate, AACS cannot ensure that all access to explicit, inappropriate or unlawful materials will be completely blocked. However, intentionally accessing such resources is inappropriate and will result in disciplinary action and/or denial of privileges.

Student Training
AACS shall provide, at least once per school year, training to students regarding safety and the internet. This training shall include information about this Policy as well as additional information regarding appropriate online behavior, including proper interactions with other individuals on social networking sites and in chat rooms. The training shall also include information regarding cyberbullying and appropriate responses to cyberbullying.

AACS Email Accounts
AACS provides users with email accounts for the purpose of school-related communication. Use

of AACS email accounts for personal, non-school-related purposes is prohibited. AACS reserves the right to revoke permission to use an AACS email account at any time for any reason.

Users are expected to utilize email accounts in an appropriate manner and in a manner that is mindful of the personal and network security risks. Students may not send personal information to unknown individuals or individuals that they have met online. Users should not attempt to open files or follow links from unknown or untrusted origins. Users should use appropriate language. Students are prohibited from communicating via email in a manner that violates the Code of Conduct, AACS policy or the rules/requirements of an individual teacher.

Email usage may be monitored and archived. Users are reminded that they have no expectation of privacy with regards to emails created/received on AACS's system. For safety reasons, AACS may periodically conduct searches of AACS email accounts. AACS has sole discretion to access, maintain and/or destroy emails sent and/or received from an AACS account as it deems necessary/appropriate.

Board members may be issued AACS email accounts. AACS monitoring and searches, as set forth in this Policy, shall not apply to these accounts. Where AACS has reason to suspect unlawful activity occurring through the use of a Board member's email account, it shall be immediately reported to the Executive Director, who shall make a determination regarding what action is necessary, including potential referral to law enforcement. Credible suspicions of unlawful activity by Board members shall always be referred to law enforcement. The Executive Director shall contact AACS Solicitor prior to taking any action regarding a Board member's email account.

Student Use of Social Media Prohibited
Students are prohibited from using social media, as defined in this Policy, on AACS's network, during school hours and/or during school-sponsored activities unless such use is for a school project sanctioned by a teacher with prior approval from the building principal. Use of AACS collaborative-content sites is permitted.

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.
If a user believes or suspects that a computer or mobile device he/she is using might be infected with a virus, the user must immediately alert IT. Users should never attempt to remove the virus themselves or download any programs to help remove the virus.

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, the following guidelines must be followed:

1. Users may not reveal their passwords to another individual.

2. Users may not to use a computer that has been logged in under another user's name. If a previous user has not logged off, the current user must immediately log out and then log back in under his/her own name and password.

3. Users must create passwords that follow the school requirements for minimum characters and required letter/number combinations.

4. Users must change their passwords every six (6) months or when prompted by AACS.

AACS will regularly review the security of the system and mandate or recommend, at regular intervals and where a potential security threat is posed, that Users change their passwords.

Unauthorized Access
Unauthorized access, including hacking and logging into the network using another individual's username and password, is strictly prohibited and will result in discipline and denial of privileges. Such unauthorized access may also result in a referral to law enforcement and potential criminal charges.

Disabling of Filters for Research Purposes
Internet filters may be temporary disabled to enable a particular user unrestricted access to a website for legitimate research purposes. In such instances, a building administrator must be present during the entire period of unrestricted research.

Personal Student Information
Users are prohibited from publishing on the internet or otherwise disseminating the personally identifiable information of students. Students who publish to the internet personally identifiable information about other students on the school's network, during the school day, on school grounds or during school-sponsored activities may be subject to discipline and/or loss of privileges. AACS employees are required to comply with the Family Rights and Privacy Act (FERPA).

Downloads
Users are not permitted to download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff. Students are not permitted to download any file types, including images, photos, video or audio files, without permission from a teacher or building administrator. For the security of AACS's network, users should download such files only from reputable sites and only for educational purposes.

Plagiarism
Users may not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users may not misrepresent themselves as an

author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Copyright
Federal and state copyright laws govern and restrict the permissible use of all material accessed on AACS's network and the internet.

Personal Safety
Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet allows potential perpetrators to interact anonymously with students, which bears associated risks. Users should carefully safeguard the personal information of themselves and others. Users should never agree to meet in real life, without parental permission, someone they initially met online .

Any student who receives threatening or unwelcome communication should report such communication immediately to a teacher or administrator. Employees should report such communications to their immediate supervisors or, if the communication is from such supervisor, directly to the building principal or AACS -level administrator. Students who receive threatening or unwelcome communication while at home or off-campus are encouraged to immediately report it to their parents or other adult. Harassing, threatening or bullying communications made by AACS staff or students to other staff or students should be reported to AACS administration regardless of whether such communication was received during school hours, on school grounds or at school functions.

AACS Monitoring of Internet and Network Usage and Activity
AACS reserves the right to monitor and log User activity on AACS's network. Users shall have no expectation of privacy for activity on AACS's network. User network passwords prevent unauthorized individuals from accessing AACS's network without permission, however, such passwords are not required for authorized IT administrators and other AACS administrators to access an individual account.

Cyberbullying
Cyberbullying and online harassment is unacceptable behavior. Cyberbullying and online harassment occurring on AACS's network, during the school day, on school grounds and/or at school events will not be tolerated. Cyberbullying and online harassment can occur through email, texting, social media, etc. It can occur in the form of direct harassment/bullying; threatening communications; falsely impersonating another individual online with the intent to harass, embarrass, or otherwise psychologically harm another individual; etc.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, on AACS's network could result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Students should remember that their online activities on AACS's network and/or on AACS technology may be monitored and retained.

Adoption Date:	09/15/2014
Revision Date(s):	

Prohibited Content
Users may not access materials that are obscene, contain child pornography or are harmful to minors. The building administration shall have the responsibility of determining whether content falls within these categories. Users are encouraged to use common sense and good judgment when accessing materials online. Employees who wish to access online content for educational purposes but are not sure whether such content falls within the above definitions of "obscene," "child pornography" or "harmful to minors" are required to consult with the building principal.

The dissemination of explicit sexual materials to minors is unlawful and will be subject to discipline and possible criminal sanctions. This includes, but is not limited to, obscene materials, as set forth in 18 Pa. C.S.A. 6312.

Examples of Acceptable Use

Users should:

- Use the Internet, network resources, and online sites in a courteous and respectful manner.
- Recognize that among the valuable content online, there is also content unverified, incorrect, or inappropriate. Users should use trusted sources when conducting research via the Internet.
- Use school technologies for school-related activities.
- Follow the same rules for respectful, responsible behavior online that that are expected for offline behavior.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if of any threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of themselves and others.
- Help to protect the security of school resources.

Examples of Unacceptable Use

Users may not:

- Engage in illegal activity.

- Engage in non-AACS -related for-profit activities on AACS's network.
- Participate in online gaming or gambling.
- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Use AACS email to send hate mail, make threats, make discriminatory remarks against peers or AACS employees, use offensive, inflammatory or inappropriate language.
- Distribute, reproduce or otherwise use copyrighted materials without authority/permission.
- Circumvent or attempt to circumvent the school's safety measures and filtering tools.
- Use AACS email or AACS network to send spam or chain mail.
- Plagiarize content found online.
- Post or electronically communicate personally-identifying information, about themselves or others.
- Agree to meet in real life someone who the user met online and does not know in real life.
- Use language online that would be unacceptable in the classroom.
- Attempt to hack or access sites, servers, or content or otherwise improperly access AACS's network or any other network or website.
- Access and/or disseminate obscene, sexually suggestive, sexually explicit, obscene or pornographic materials, including child pornography.
- Intentionally use, retrieve or modify files, passwords and/or data belonging to other users.
- Impersonate another user (fictional or otherwise) online.
- Load or use unauthorized games, programs, files or other electronic media.
- Disrupt the work/programs/work product of other users.
- Destroy, modify, or access without authorization network hardware, software and/or files.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Users should understand that information that is posted on a 3rd party website is likely irretrievable and that electronic files and information can be spread very quickly to large numbers of people. Users should not to post anything online that they would not want parents, teachers, peers, employers or future colleges or employers to see.

Incidental Personal Use by Employees

Employees may engage in incidental personal use as a privilege, as defined in the "Definitions" section, above. Such use must be limited to occasional use only and must comply fully with the terms of this Policy and any accompanying Administrative Regulations. AACS reserves the right to prohibit incidental personal use by all or specific employees for any reason, including

where there is a history of misuse, where such use becomes a burden for AACS's technology or where enforcement of the incidental personal use requirements become too cumbersome. Where incidental personal use is prohibited by a specific employee or group of employees, AACS must provide notification to such employee(s) of the prohibition of such use.

The Board herein grants the Executive Director the authority to limit, through the development of administrative regulations, incidental personal use to specific times of the school day or to eliminate such privilege entirely, as the Executive Director deems appropriate.

Expectation of Privacy

Students and staff are reminded that they have no expectation of privacy when using school technology, its email system or its network.

All files/information uploaded to or through the school's network shall be subject to search and/or deletion/removal. Users shall have no expectation of privacy for such files/information.

Limitation of Liability

AACS makes no warranties of any kind, either expressed or implied, that the functions or services provided by or through AACS's computer network systems will be error-free or without defect. AACS will not be responsible for damage or harm to persons, files, data, or hardware due to use of AACS's network.

While AACS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

AACS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Policy

The user shall be responsible for damages to equipment, systems and software resulting from deliberate or willful acts. AACS reserves the right to hold students/employees responsible for damage that occurs due to negligence.

Adoption Date:	09/15/2014
Revision Date(s):	

Consequences of violation of this policy may include:

- Temporary or permanent suspension of network, technology, or computer privileges;
- Disciplinary action, which could include detention, suspension from school-related activities, suspension from school and/or expulsion;
- Parental notification of student misuse/violation;
- Reporting of suspected illegal action to law enforcement;
- Employment disciplinary action for employee violation/misuse;
- Legal action and/or prosecution.