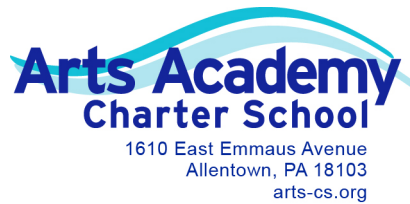


Adoption Date:	09/15/2014
Revision Date(s):	



Board Policy 9.1.1

Acceptable Use of School Technology

Purpose

The Arts Academy Charter School (herein referred to as AACCS) 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, AACCS provides access to computers, mobile devices and other technology. AACCS is committed to working with parents and students to assist them in maximizing and understanding the educational potential of available technology, using such technology responsibly, and understanding the inherent risks posed by some forms of technology.

Definitions

Incidental Personal Use – This term refers to use of school technology by AACCS 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.

Network – The term “network,” for the purposes of this Policy, includes AACCS’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 AACCS’s server. The term also expressly includes any system linking two (2) or more school electronic devices.

School Devices / School Technology – Under this Policy includes, but is not limited to, desktop computers, mobile computers or devices (including, but not limited to, laptops, netbooks, tablet PCs, etc.), videoconferencing capabilities, smartboards, printers, scanners, software, cables, modems, data storage devices (including, but not limited to, DVDs and CDs, flash drives, external hard drives and CD-Roms, etc.) specialized electronic equipment used for students’ special educational purposes, global position system (GPS) equipment, school personal digital assistants (PDAs), school cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities), other school wireless devices, two-way radios/telephones,

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

beepers, paging devices, laser pointers and attachments, and more. As new technologies emerge, AACS will attempt to provide access to them. This policy covers any and all school or leased hardware, software, or other technology owned by AACS.

Guidelines and Requirements

AACS shall not tolerate illegal activity, cyber-bullying or other improper activity on school technology, illegal or otherwise.

Non-AACS-Related Uses of School Technology

All student use of technologies provided by the school are intended for educational purposes and may not be used for purposes unrelated to AACS education. School technology may not be used for non-educational purposes.

With the exception of limited, incidental personal use, as defined and regulated herein, employee use of AACS technology is limited to those tasks that are within the scope of the school employee's responsibilities.

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.

Privacy

Users of school devices have no expectation of privacy on such devices, including with internet access and access histories, and AACS may confiscate and/or search school device at any time.

School Mobile Devices

AACS may provide users with mobile computers or other devices to promote learning outside of the classroom. Users are required abide by the standards set forth in Bd. Pol. 815.2 for appropriate use of the internet when using school devices off the school network.

School-owned mobile devices are issued for professional use and may not be used for personal purposes. If a user is not sure whether a particular use is appropriate under this Policy, he/she must seek an opinion from his/her building principal.

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

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users will be financially accountable for any damage resulting from loss, theft, negligence, mishandling or misuse.

Users shall have no expectation of privacy on school mobile devices.

Use of school-issued mobile devices off the school network may be monitored or tracked by location. All voice, data and call logs will be fully accessible by AACCS as well as any other available data regarding the use of the device that may have been electronically collected by the device or AACCS's network.

Downloads and/or Upgrades

Users may not download to, attempt to download to or upgrade a school device without prior written permission from the building principal and/or a member of AACCS's IT staff. AACCS's IT staff is required to record all instances of written permission granted for such downloads/upgrades. Such records shall be retained for a minimum of two (2) years.

All files/information downloaded to or installed onto a school device shall be subject to search and/or deletion/removal. Users shall have no expectation of privacy for such files/information.

Security

Users are expected to take reasonable safeguards against the transmission of security threats on school devices. 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 that a computer or mobile device might be infected with a virus, immediately alert IT. Users should not attempt to remove the virus yourself 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 are 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. If a user suspects or knows that his/her password has been compromised, he/she is required to report it immediately to the building principal and IT staff.

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

Confiscation of or Revocation of Permission to Use School Technology

AACS may revoke a user's permission to use school technology at any time for any reason. Likewise, AACS may confiscate a school device at any time for reason. Use of school devices and school technology privileges shall be immediately revoked where the User has violated this Policy, Bd. Pol. 815, 815.2, 815.3, 815.4, or where the User has violated another Board Policy or the Student Code of Conduct when using school device.

Access of Illegal or Inappropriate Materials Prohibited on School Devices

Users are prohibited from accessing or downloading any content and/or materials that are prohibited by law and/or by Bd. Pol. 815.2.

Lost or Stolen Devices

Employees and students are required to immediately report any AACS technology that is lost or stolen and must fully cooperate with any associated investigation.

User Responsibility for Damage, Loss or Theft

Employees and students may be responsible for the depreciated cost of a school device that is lost or stolen due to intentional misuse, gross negligence or recklessness.

Limitation of Liability

AACS will not be responsible for damage or harm to persons, files, data, or hardware.

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 on school technology.

Violations of Policy

Consequences of violation of this policy may include, but are not limited to:

- 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.