ACPS EMPLOYEE RESPONSIBLE USE POLICY AGREEMENT FOR COMPUTER SYSTEMS

This Agreement further explains Policy GAB/IIBEA: ACPS Responsible Computer System Use. If you have any questions about the policy or this regulation, contact your supervisor.

- ACPS employees utilize computer systems to support the mission and educational goals of the Division.
- ACPS employees understand that documents and communications created on Division equipment are the property of the Division.
- ACPS employees access the ACPS network and Internet resources respectfully with regard to language, information and resource limits.
- ACPS employees accept personal responsibility for our equipment and make every effort to afford the equipment proper care and security.
- ACPS employees value the importance and principles of digital citizenship.

All use of the Alexandria City Public Schools' computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term "computer system" includes hardware, software, data, communication lines, printers, servers, computers, the Internet, internal or external networks and any other digital device or peripherals. Technology provided by ACPS is intended for use by school personnel only. Family and friends are not authorized to use ACPS technology.

Responsible Use

Access to ACPS's computer system shall be for the purposes of education or research and be consistent with the Division's educational goals.

Limited, incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal business not occurring during instructional time, which is not otherwise prohibited by this regulation.

Initial

Digital Citizenship

In accordance with the Code of Virginia § 22.1 -70.2, Alexandria City Public Schools trains students to use best practices in Internet safety. It is the responsibility of all ACPS employees to support students, as well as be models of best practices in internet safety and appropriate computer use. Internet Safety must be taught to and practiced by all students in grades K through 12.

Initial

Electronic Mail

ACPS owns and controls the ACPS electronic mail system. Electronic mail is not private and is monitored. Employees must use their ACPS email when communicating as an ACPS employee with staff, parents and students. ACPS mail should be used for professional correspondence only. Unauthorized access to an electronic mail account by any employee is prohibited. Employees shall be held personally liable for the content of any electronic message they create. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file. Employees shall not forge, intercept or interfere with electronic mail messages.

Initial

Copyright and Terms of Use Violations

Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any federal, state or local law is prohibited.

Downloading or unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which ACPS or the end user does not have an active license is also prohibited. Terms of Use must be followed when using digital resources.

Software/Applications Initial

ACPS supports and authorizes the use of a variety of software applications. A list of approved software can be found in the Virtual Teaching and Learning Course in Canvas. Downloading or installation of unauthorized software is prohibited. End users cannot install, run, or download software or modify configurations on network connected computer systems unless directly authorized by Technology Services. When using online applications, Terms of Use Agreements must be followed.

Installation of network connected computers, maintenance, repair, updates including hardware and software, must be approved, directed, and completed by Technology Services.

Offensive Materials Initial

Submitting, posting, publishing, storing, printing, downloading, transmitting, viewing or displaying files or messages (text, sound, still, or moving graphics, or any combination thereof) that are pornographic or are obscene, as defined in the Code of Virginia §18.2-372; use language, sounds, or imagery which is lewd or patently offensive (including "sexually explicit visual materials" as defined at the Code of Virginia §18.2- 374.1); or degrade others is prohibited. (The administration invokes its discretionary rights to determine suitability in particular circumstances.)

Initial

Harassment/Bullying

Harassing another person by transmitting or posting material on any website/electronic medium which is threatening, or is intended to coerce or intimidate is prohibited.

Transmitting or posting material intended to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or making any suggestion or proposal of an obscene nature; or threatening any illegal or immoral act is prohibited.

Initial

Vandalism

Employees are prohibited from vandalizing any computer system by creating, downloading or spreading viruses. Intentional destruction of data or any part of the computer system by any means is also prohibited.

Attempting to modify system facilities, downloading, installing, or transmitting viruses from email attachments or any other source, illegally obtaining extra resources, or attempting to subvert the restrictions associated with any computer system, computer account, network service, or personal computer protection software is prohibited.

Initial

Non-school Related Business

Using the ACPS equipment or network for personal or private financial gain or advertising, solicitation or business activity not on behalf of Alexandria City Public Schools is prohibited.

Users shall not post professional ACPS contact information for non-school related activities.

Communicating through ACPS email or any other ACPS medium with other school users or outside parties to solicit, advocate, or communicate the views of an individual or non-school-sponsored organization including political and religious material; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether for profit or not for profit, is prohibited.

No employee shall knowingly provide names, email addresses, or other personal information to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes.

Employees who are uncertain as to whether particular activities are acceptable shall seek further guidance from their supervisor or the Chief Technology Officer.

Initial

Security

Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately.

ACPS expects all users of ACPS computer equipment to make every effort to utilize the equipment with proper care and security. In the case of portable equipment or equipment assigned to individuals for use off-site or at home, the user must accept personal responsibility for said equipment, and must accept the risk of theft, loss, or damage due to negligence. If equipment is stolen, a police report should be filed immediately and a copy of the report must be submitted to Technology Services. In the event of loss, theft or damage, please notify the Help Desk immediately.

Employees may not:

- Send ACPS proprietary and classified information to unauthorized persons, or post this information outside of ACPS;
- Distribute any school interior maps, floor plans, or written descriptions of interior floor plans on Web pages, camera locations, or other information that could compromise school security; or
- Gain unauthorized access to resources or entities including educational systems, government agencies or privately owned businesses.

Authorized users are responsible for the security of ACPS passwords and accounts. Passwords are considered secret and are not to be shared under any circumstance. Individual user passwords must never be embedded into a document, application, or process, i.e., "Remember me on this computer."

Users shall not read, modify, post or delete materials owned by others without authorization. Materials include but are not limited to documents, movies, graphics, pictures, and presentations.

Users are responsible for following the recommended virus protection procedures.

ACPS employees may not use non-ACPS hardware to access the ACPS network. This does not include remote access to web-based resources (i.e., student information systems, professional learning applications, email, etc.).

Permission should be secured from Technology Services before allowing outside speakers, presenters, etc. to connect equipment to the ACPS network.

Initial

Liability

The School Board makes no warranties for the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information or service interruptions. The school division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs or damages arising out of any violation of these procedures.

Initial

Resource Conservation

Resources, including file space and print services, should be used for legitimate instructional purposes. Personal files, including but not limited to, pictures, music, and video, should not be stored on or streamed through ACPS computer systems or file servers.

Initial

Charges

ACPS assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone or long distance charges. ACPS may charge fees associated with lost, stolen or mistreated hardware.

Initial

Enforcement

ACPS will install software on ACPS computers having Internet access to filter or block Internet access through such computers to child pornography and obscenity.

Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, including replacement costs, administrative action; employee discipline up to and including dismissal; and criminal prosecution under applicable local, state and/or federal law.

_____

I understand and agree to abide by the school division's Responsible Computer System Use Policy (GAB/IIBEA) and Regulation (GAB-R/IIBEA-R). I further understand that should I violate the Responsible Use Policy or Regulation, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Employee Signature_____ Date _____

Revised: July 2, 2012
Revised: November 16, 2015
Revised: August 20, 2020