RESPONSIBLE STAFF USE OF TECHNOLOGY

Use of the Albemarle County Public School Division's ("Division") technology shall support the educational mission and operations of the Division as well as the varied instructional needs and developmental levels of staff and students.

Each student, their parent/guardian and staff shall be encouraged to review the Responsible Use Policy. The failure of any student or employee to follow the terms of this policy or accompanying regulation may result in disciplinary action.

To promote educational excellence, the School Board ("Board") provides technologies by facilitating resource sharing, innovation and communication. The term technology includes computer hardware, peripheral devices, software, data, the internet (including web-based tools and resources) and internal and external networks.

All use of the Division's technology must be in support of education and/or research, or for legitimate school business. The Division reserves the right to monitor any activity, communication, file creation or storage that utilizes Division technology resources. An individual account or activity may be monitored without notice.

It shall be the responsibility of all ACPS staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the internet in accordance with this policy and the Children's Internet Protection Act.

The Division operates a technology system that monitors and blocks internet access to the following in compliance with the Children's Internet Protection Act (CIPA):

a) child pornography as defined in Va. Code
b) obscenity as defined in Va. Code
c) material the Division deems harmful or inappropriate to minors as defined in Va. Code
d) student usage that indicates possible health and/or safety concerns

Student personally owned laptops may not be used during school hours unless approved by the school principal. Use of personal communications devices (including cell phones, watches, and other personal devices with cellular service) is allowed as outlined in Cell Free Education JFCP. The Division's technology staff will not maintain or service personal technology devices.

In support of the educational mission and operations of the Division the following actions will be subject to disciplinary action, including criminal prosecution, if appropriate:

- sending, receiving, viewing, or downloading illegal material
- intentional destruction of, intrusion into, or interference with any part of technology systems by any means

The Division Superintendent/Designee shall establish administrative regulations for technology regarding the appropriate uses, ethics, and protocols and will review the administrative regulations as necessary. Regulations shall include:

a) Instruction regarding digital citizenship and web safety for students that is required as part of the Division's mandated curriculum.

b) The risks of transmitting personal information on the internet and the importance of privacy protection.
c) The enforcement of copyright laws on written materials, photographs, music, and videos posted or shared online.
d) Educating, supervising, and monitoring appropriate usage of the online computer network and access to the internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.
e) Providing internet safety and digital citizenship resources to their school community including online courses, in person programs, resource hubs, and digital guides.

The Board and Division shall not be responsible for any information that may be lost, damaged or unavailable when using ACPS technology systems or for any information retrieved. Additionally, the Board and Division shall not be responsible for any damages to a person from use of the computer or technology systems, including loss of data, non-delivery or missed delivery of information, or service interruptions. Furthermore, the Board and Division shall not be responsible for any unauthorized charges or fees resulting from access to the technology systems, including telephone, data, or long- distance charges.

Adopted:	August 26, 1996
Amended:	February 22, 1999; April 22, 2004; May 24, 2007; May 27, 2010; August 8, 2013; August 8, 2019; January 13, 2022
Equity Review:	August 8, 2019

Legal Ref.:	18 U.S.C §§1460, 2256. 47 U.S.C. § 254 Virginia Code, 1950, as amended, §§18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2, 22.1-78.
Cross Refs:	JFC, *Student Conduct* JO, *Student Records* JFCP, *Personal Device-Free Education* [TO BE LISTED IF APPROVED] IIBE, *Responsible Student Use Technology*

RESPONSIBLE USE REGULATIONS FOR STAFF

The Division expects staff to exercise personal responsibility when using technology and to model ethical uses of technology.

Administrative Guidelines for Staff Acceptable Use of Technology

1. Staff will use technology resources in a responsible, ethical and legal manner. Unethical or illegal activities include, but are not limited to: knowingly spreading viruses and/or compromising your ACPS network account, violating copyright laws, using unauthorized software, unauthorized impersonation of another person, unauthorized entry, intentional access to inappropriate content, and/or destruction of computer systems and files.

2. Any electronic, online, or social media messaging interaction with students or families must comport with the Standards of Conduct policy.

3. Staff should understand that any information generated, stored, or sent through Division technology resources is considered to be the same as written documentation and may be subject to requests under the Virginia Freedom of Information Act and disclosure pursuant to subpoenas, search warrants, court orders, and discovery requests.

4. Staff shall not use, create, distribute, import, or otherwise promote illegal, offensive, obscene, libelous language, pictures, or other similar material on any computer, technology resource, network or the internet.

5. Staff shall not respond to harassment encountered on any technology system, but shall report any such activity to the appropriate supervisor, administrator, or Human Resources immediately.

6. Division employees who are responsible for the safety and supervision of students must follow guidelines established by the technology and/or Human Resources department regarding technology investigations.

7. Any employee who identifies a security problem must notify the technology department. The employee shall not demonstrate the problem to others unless requested to do so by an authorized representative. Any employee who attempts or causes a breach to the system is subject to disciplinary or legal action.

8. Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with Board policy, is limited in amount and duration, and does not impede the ability of the employee or other individual to meet the Board's objectives or otherwise fulfill their job responsibilities. The Division may revoke or limit this privilege at any time.

9. Staff shall not use Division technology systems for personal, non-Division purposes to solicit, proselytize, advocate or communicate the views of an individual or of non-

school sponsored organizations.

10. Staff shall not use Division technology systems for private financial gain, including the conduct of commercial activity for any business in which there is a personal interest, or for advertising or solicitation purposes.

Employee Social Media Accounts

- Staff are strongly discouraged from connecting with students and their families via social media. If choosing to do so employees at all times should consider the potential impacts and perceptions that can result from electronic communications and use sound judgement.

- Staff members should be aware of personal social media content that may impact their ability to perform job duties as an ACPS employee.

- This policy does not prohibit the Board and its agents from viewing information about a current or prospective employee that is publicly available.

Personally-Owned Devices

- Employees in positions that require access to a cell phone are provided one by the School Division. Employees are advised to use that device for work-related communications. No stipend is provided for use of personal devices in lieu of School Division-owned devices.
- ACPS issued laptops or desktops shall be used for school division work unless approved by the Department of Technology. Staff requesting to use a personal device should enter a technology support ticket to begin the request process.
- Possession or use of personal electronic devices must not in any way disrupt the educational process in the Division, endanger the health or safety of the employee or any other person in the Division, impinge upon the rights of others at school, or involve illegal or prohibited conduct.
- Employees using personal electronic devices for work purposes must follow the same rules that apply to the use of Division-provided technology. The Division administration may involve law enforcement if the Division has reasonable suspicion that the device has been used for an illegal purpose or for a purpose that causes harm to others.
- Personal devices used for school division business may be subject to requests under the Virginia Freedom of Information Act and disclosure pursuant to subpoenas, search warrants, court orders, and discovery requests.

Employee Use of Technology Resources for Instructional Purposes

Staff members supervising students' use of technology must take reasonable steps to ensure that students understand and follow the requirements of policy IIBE and all applicable Board policies.

1. Educators shall implement digital citizenship curriculum as outlined in the division's broader goals, especially in the areas of:

a. Media Balance & Well Being: Strategies for developing screen time habits which promote positive mental health
b. Privacy and Security: Strategies for keeping personal information and data safe and protected
c. Digital Footprint & Identity: Understanding the permanency of content posted online, and cultivating a positive digital identity
d. Relationships & Communication: Strategies for developing healthy relationships in online spaces
e. Cyberbullying, Digital Drama, and Hate Speech: Strategies for recognizing and reporting unkind behavior witnessed in online spaces
f. Media Literacy: Understanding copyright and intellectual property, and discerning truth vs misinformation online

2. Educators should be mindful when teaching with technology to ensure activities align with strands of the Digital Learning Integration Standards (empowered learning, creative communication, global collaboration, knowledge constructing, innovative design, computational thinking, and digital citizenship).

3. Educators should emphasize and model healthy digital wellness habits for students by employing various strategies. Examples may include establishing healthy screen time limits, developing activities that support emotional, physical, social, and cognitive development, or developing blended learning spaces in the classroom that support increased engagement, physical movement, and collaboration.

4. Recommend safe search strategies and resources which meet the curricular needs of the assignment and the developmental level of the student.

Staff members should also seek to prevent student access to material that the Division deems to be harmful to juveniles, and as defined in § 18.2-390 of the Code of Virginia through instructional design. Staff should:

- only use Division-provided and/or vetted instructional resources, tools, and systems. Teachers should proceed with caution and be fully aware of both the Terms of Service and Privacy Policy before using with students or downloading onto Division property.

- request an unapproved resource to be considered as a vetted resource via the Department of Technology's website before using it with students. Policy IIAA provides staff key parameters to guide the selection of learning resources.

- provide supervision for students accessing technology resources through intentional classroom management strategies and use of Division provided systems. Employees shall consider the developmental stage of their learners when determining the appropriate level of supervision.

- minimize student data collected, teachers shall also ensure that students use only their first name and last initial when creating an account for any approved web-based

activities. Some resources may include age restrictions, or require parent/guardian permission to use.

Confidentiality of Personally Identifiable Student and Employee Data

1. Employees shall adhere to all school and Division policies and regulations, and state and federal laws, including the Family Education Rights and Privacy Act (FERPA) regarding confidential information. Employees may not share, or provide access to, personally identifiable student educational information, personally identifiable employee information, or any other Division confidential information with individuals not authorized to receive such information.

2. Whether using Division technology resources at a worksite, or at other locations, or while using portable communication devices, employees must use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential and secure.

3. Staff shall not create accounts for students of web resources that have not been vetted or purchased by the Division.

4. Account access to systems containing confidential data will only be granted to employees who meet the conditions of Board Policy JO – Student Records, Board Policy GBL – Personnel Records and other Board policies, and local, state and federal laws as applicable to the particular system. The use of such accounts must comply with all applicable laws and policies.

Web Publication

1. Web site content published by employees using ACPS resources must adhere to all applicable Division and federal requirements.

2. With appropriate notification and/or permission, student projects and other material relating to individual students may be published on the Division's website, social media or through other services selected by Division staff. In all cases, content must be appropriate and relevant to the mission and the business of the Division. In no case, shall information about a student, such as home phone number, personal e- mail address, etc., be published.

Purchasing/Commercial Activities

1. All technology-related purchases or product demonstrations, including consultant and development services, must be approved by the Chief Technology Officer or designee.

2. Use the Department of Technology Purchasing site for all technology purchases and requests to ensure system compatibility and effective support.

Acceptable Use of Electronic Communication Systems by Employees

Electronic communication systems continue to evolve. These systems may include, but may not be limited to systems such as: E-mail, Mass Messaging systems, Chat Messaging systems, texting, and phone calls. ACPS staff members should abide by the following guidelines when using ACPS systems.

1. Employees should use ACPS provided communication systems and tools for communication with families and students.

2. Whenever possible, staff should communicate with groups of students. When necessary to communicate with an individual student, ACPS strongly recommends the student's parent/guardian be copied.

3. When employees use communication systems for confidential matters or privileged communications, such as student education records, they shall take appropriate measures to ensure confidentiality.

4. Global Distribution Lists exist to facilitate communication between and among specified groups of staff. Sending mass communications to Division employees or outside parties for non-school purposes is prohibited. Use of Global Distribution lists should be purposeful and limited to work-related matters that pertain to the entire recipient list.

5. Staff shall follow normal communication etiquette when using communication systems.

    a. Employees shall utilize an email signature that appropriately identifies them in the following template: Name, Job Title, School/Department. Optional School Division, Phone Number, Work Address, Work Website Link. Signature blocks shall not include any personal slogans, quotes, aphorisms, links to non-Division websites, or any other personal messages.

    b. When receiving attachments or links via E-mail or other systems, employees shall use caution if it comes from an unidentified or questionable source. When in doubt, consult with the technology department prior to opening an attachment or clicking a suspicious link.

    c. Users may not create, or forward any attachments using E-mail or other systems that are known or suspected to contain viruses unless it is being forwarded to a Division technology professional for evaluation purposes.

6. Employees with e-mail accounts are responsible for maintaining their accounts in a manner that promotes the conservation and protection of Division resources. E-mail system backups are maintained for short periods of time for the purpose of disaster recovery only. Individual users are responsible for their own backups. Communications may be subject to Virginia Freedom of Information Act inquiries.

Network Guidelines for Staff

1. Employees shall access only files and data created and maintained by them, that are publicly available within the school network and online systems, or to which they have been given authorized access. This includes, but is not limited to, files residing on assigned technology, servers, or other storage devices.

2. In an effort to keep the network operating effectively and securely, and to ensure that employees are using the system responsibly, the Division reserves the right to review the content of all Division accounts and data contained therein.

3. Employees should never share their Division assigned username and password via E-mail, text, website, verbal, written communication, or any other method. Employees are encouraged to maintain strong passwords and reset passwords at designated intervals.

Electronic Timekeeping Systems

The Division permits the use of electronic timekeeping terminals, web-based applications and devices for the tracking of compensable work time and leave balances for employees. Whenever possible, employees are encouraged to use ACPS terminals or devices for logging, viewing, and/or submission of time/leave records.

The Division discourages the use of personal devices for timekeeping. However, if necessary to use a personal device the employee must agree to the following:

1. The Division will not provide technical support or maintenance for personal devices.
2. The employee must immediately report to a supervisor any issue reporting time through a personal device and make alternative arrangements to submit time worked.
3. The Division will not purchase or reimburse employees for use of personal equipment to track work time/leave or pay for the cost of repair for any damage to such personal equipment incurred.
4. The employee accepts the software user agreement by installing the application on a personal device, which includes enabling geo-location services.

Adopted: August 8, 2013
Amended: September 10, 2015; December 13, 2018; August 8, 2019; January 13, 2022; October 27, 2022
Equity Review: August 8, 2019

Legal Ref: Code of Virginia, 1950, as amended, § 40.1-28.7:5

Cross Refs: JFC, *Student Conduct*
JO, *Student Records*
JFCP, *Personal Device-Free Education* [TO BE LISTED IF APPROVED]
IIBE, *Responsible Student Use Technology*