ACCEPTABLE USE OF TECHNOLOGY

Use of the Albemarle County Public School Division's ("Division") technology shall be consistent with the educational mission or administrative function of the Division as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The School Board ("Board") provides technologies, including the internet, to promote educational excellence by facilitating resource sharing, innovation and communication. The term technology includes hardware, software, data, communication tools, printers, multimedia devices, servers, personal computers, and the internet (including web-based tools and resources) and internal or external networks.

All use of the Division's technology must be (1) in support of education and/or research, or (2) for legitimate school business. Any communication or material using Division technology, including electronic mail or other files deleted from a user's account, may be monitored or read by Division officials without prior notice.

Division employees and students may not use Division technology services for sending, receiving, viewing or downloading illegal material via the Internet. Intentional destruction of or interference with any part of the computer system through creating or downloading computer viruses or by any other means is prohibited and will be subject to disciplinary action, including criminal prosecution, if appropriate.

The Division operates a technology protection tool that monitors or blocks internet access to the following, in compliance with the Children's Internet Protection Act (CIPA) as codified by 47 U.S.C. 254(h) and (l):

(a) child pornography as defined in Va. Code § 18.2-374.1:1 and/or 18 U.S.C. § 2256;

(b) obscenity as defined in Va. Code § 18.2-372 and/or 18 U.S.C. § 1460; and material that the Division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;

The Division Superintendent/Designee shall establish administrative procedures for technology regarding the appropriate uses, ethics, and protocols for staff usage, and staff responsible for oversight of student usage of technology. The Division Superintendent/Designee will review and update, as necessary, the administrative procedures at least every (2) years. The procedures shall include:

(1) provisions establishing that the technology protection tool is enforced during any use of the Division's computers by students;

(2) provisions establishing that the online activities of students will be monitored;

(3) provisions designed to educate students about appropriate online behavior, including but not limited to, interacting with other individuals via website, social media platform, other online forums, and cyberbullying awareness and response;

(4) provisions designed to prevent unauthorized and unlawful online access by minors;

(5) provisions prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding students; and

(6) education regarding digital citizenship and web safety for students that is integrated into the Division's instructional program.

Each employee shall be given the opportunity to acknowledge the Acceptable Use Policy. The failure of any student or employee to follow the terms of this policy or accompanying regulation may result in disciplinary action.

The Board and the Division shall not be responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the Board and Division shall not be responsible for any unauthorized charges or fees resulting from access to the computer system, including telephone, data, or long-distance charges.

Adopted: August 8, 2013
Amended: September 10, 2015; December 13, 2018; August 8, 2019; January 13, 2022; October 22, 2022
Equity Review: August 8, 2019

Legal Refs: 18 U.S.C. §§ 1460, 2256.
47 U.S.C. § 254.

Code of Virginia, 1950, as amended, §§ 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2, and 22.1-78.

Cross Refs: GBC, *Standards of Conduct*
GBL, *Personnel Records*
IIBE, *Acceptable Use of Technology*
JFC, *Student Conduct*
JO, *Student Records*

ACCEPTABLE USE OF POLICY REGULATION

Expectations for Using School Technology

- The Division expects staff to exercise personal responsibility when using technology.
- The Division expects staff to exhibit ethical uses of technology.
- The Division expects staff to use technology to enhance productivity and the learning environment.

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.
- Personal technology devices are permitted for use, but not recommended because they cannot be supported.
- Personal technology devices are only permitted to use ACPS-PUBLIC wireless network for security purposes. Special exceptions may be made for documented medical reasons.
- 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 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.

Monitoring the Use of Technology

Although the Division does not routinely monitor an individual's usage of the Division's technology, there should be no expectation of privacy. The normal operation and maintenance of the Division's technical infrastructure and services requires that data and electronic communications are routinely backed up, and programs or other devices are employed to maintain the functionality, integrity, or security of the network infrastructure. 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.

The Division reserves the right to monitor any activity, communication, or file creation or storage that utilizes Division technology resources. An individual user's account or activity may be monitored, without notice.

The Division provides users with access to online educational services and websites through contracts with educational companies and vendors. When applicable, users may be provided with a username and password to access educational content on these websites.

Liability

The Board and Division makes no warranties for the computer system it provides. The Board and Division 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 Board and Division deny any responsibility for the accuracy or quality of external information obtained through the computer or technology systems. The user agrees to indemnify the Board and Division for any losses, costs, or damages incurred as a result of any misuse of equipment and systems or a violation of these regulations.

Administrative Procedures for Staff Acceptable Use of Technology

1. All employees using technology resources must follow and enforce this policy in accordance with all relevant Board and school policies and codes of conduct.

2. Users will use technology resources in a responsible, ethical and legal manner. Unethical or illegal activities include, but are not limited to: knowingly spreading viruses, violating copyright laws, using unauthorized software, impersonating another user, unauthorized entry, and/or destruction of computer systems and files.

3. Users should understand that any information generated, stored, or sent through Division technology resources, including personal devices used in place of Division provided technology, is 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. Users 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. Users shall not respond to harassment encountered on any technology system, but shall report any such activity to the appropriate supervisor or administrator immediately.

Personal Use of Technology Resources by Employees

1. In accordance with Board policy GBC, Standards of Conduct, Division employees may not abuse their access to technology resources.

    a. Abuse may consist of either excessive or unacceptable use. Generally, a use is unacceptable if it conflicts with the purpose, goal, or mission of the Division or individual school or department's purpose, goal, or mission or with an employee's authorized job duties or responsibilities.

    b. 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. The Division may revoke or limit this privilege at any time.

2. 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 except through means that have been provided specifically for such purposes (e.g., County Bulletin Board). However, the Division recognizes that employees have certain rights to speak out on matters of public concern, and this provision shall not be construed to restrict or prohibit the legal rights of employees to engage in speech that is protected under federal or state laws.

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 this policy and all applicable Board policies.

<u>Digital Citizenship Requirements</u>

Staff members assigning or permitting student internet use shall:

1. Deliver instruction regarding internet safety utilizing materials provided through the

Division's Digital Citizenship Curriculum. See Digital Citizenship Curriculum on our Department of Technology's Website.

Topics to be addressed include:

a. Content of this Policy and Regulations

b. Generally accepted rules of network etiquette and safety

c. Copyright guidelines

d. Internet Safety

e. Other acceptable use/safety related topics

f. Respect for use of time and resources, including following replacement prescribed for division technology

g. Evaluating sites for appropriateness and validity

h. Discriminating among types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity.

2. Seek to prevent access by students to material that the Division deems to be harmful to juveniles, and as defined in § 18.2-390 of the Code of Virginia.

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

4. Use Division-provided, vetted instructional resources, tools, and systems before considering free options. Given the abundance of free online educational tools, 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. Please refer to the Department of Technology website to request a resource to be considered as a vetted resource. Policy IIAA provides staff key parameters to guide the selection of learning resources. Web resources could be collecting student data and personal information as well as include age restrictions. Teachers shall also ensure that students use only their first name and last initial when participating in these web-based activities. Parental/guardian permission may be required.

5. Provides supervision for students accessing technology resources. Employees shall consider the developmental stage of their learners when determining the appropriate level of supervision.

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 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 without notifying the parents of the intended use and a copy of the privacy statement as required by federal law, thereby allowing guardians to opt out for their student.

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, 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 content published by employees 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 Divisions staff. In all cases, content must be appropriate and relevant to the mission and the business of the Division. Consent is obtained when a parent acknowledges the Student Acceptable Use Policy IIBE. In no case, shall information about a student, such as home phone number, personal e-mail address, etc., be published.

Commercial/Purchasing Activities

1. All technology-related purchases or product demonstrations, including consultant and development services, must comply with the guidelines established by the Chief Technology Officer.

2. Staff shall not use Division technology 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.

Acceptable Use of E-Mail by Employees

1. 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.

2. When employees use email for confidential matters or privileged communications, such as student education records, they shall take appropriate measures to ensure confidentiality and to maintain the appropriate privilege.

3. Staff shall report any incident of harassment or any other unauthorized or inappropriate use of technology to the technology department and/or the building or department administrator.

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

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

    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 E-mail attachments or links, 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.

    c. Users may not create, or forward any e-mail attachments 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. E-mail communications may be subject to Virginia Freedom of Information Act inquiries.

Network Guidelines for Staff

1. Users 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 working properly and to ensure that users 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 email, text, website, verbal, or written communication. Employees are encouraged to maintain strong passwords and reset passwords at designated intervals.

Access to Employee Social Media Accounts

The Division does not require current or prospective employees to disclose the username and password to the employee's personal social media accounts or to add an employee, supervisor, or administrator to the list of contacts associated with the employee's personal social media account.

If a Board member or a Division employee inadvertently receives an employee's username and password to, or other login information associated with, the employee's personal social media account through the use of an electronic device provided to the employee by the Board or a program that monitors the Board's network, the Board will not be liable for having the information, but will not use the information to gain access to the employee's social media account.

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

This policy does not prohibit the Board from requesting an employee to disclose the employee's username and password for the purpose of accessing a personal social media account if the employee's social media account activity is reasonably believed at the initiation and in determination of the scope of the investigation to be relevant to a formal investigation or related proceeding by the Board of allegations of an employee's violation of federal, state or local laws or regulations or of the Board's written policies. If the Board exercises its rights under this paragraph, the employee's username and password will only be used for the purpose of the formal investigation or related proceeding.

Electronic Timekeeping Systems

The Division may permit the use of electronic terminals and web-based applications for the tracking of compensable work time and leave balances for employees. Not all employees may use all electronic means of tracking time.

The Division may allow, but not require, the use of employee personal devices for such purpose. Personal devices are permitted to use ACPS-PUBLIC wireless network or elect to use their own personal data plan. If an employee so chooses to use personal equipment for the logging, viewing, and/or submission of time/leave records, he/she must acknowledge and 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