REGULATION ANNE ARUNDEL COUNTY PUBLIC SCHOOLS

Related Entries: DI, DCA, DCA-RA, DEC, DEC-RA, DJ, DJ-RA, JCC-RAA, JCC-RAJ, JCO, JCO-RA
Responsible Office: OFFICE OF INFORMATION TECHNOLOGY, OFFICE OF HUMAN RESOURCES, DIVISION OF INVESTIGATIONS, DIVISION OF SAFE AND ORDERLY SCHOOLS

TECHNOLOGY USE AND SECURITY

A. PURPOSE

To establish procedures that govern the acceptable and secure use of Anne Arundel County Public Schools (AACPS) provided technology hardware, software, information, systems, networks, and peripherals. In addition, this regulation includes governance for all technology related services under contract with AACPS, regardless of their physical location.

B. BACKGROUND

Technology resources are provided to students, employees, and, at times, approved third parties in order to advance educational and administrative purposes aligned with the goals of AACPS. Ensuring the availability, confidentiality, and integrity of AACPS technology and related data are imperative in today's digital world.

C. DEFINITIONS

1. ***Account Credentials*** – any information used specifically to gain access to a technology or system.

2. ***Least Privilege –*** only those privileges that are required for a user to fulfill the user's responsibilities.

3. ***Peripheral –*** a device or unit that operates separately from a computer, laptop, tablet, or server but is connected to it either physically or logically. Types of peripherals include external hard drives, flash drives, printers, headphones, and Bluetooth devices.

4. ***Sensitive Data –*** electronically stored or transmitted information that contains elements that may be considered personally identifiable information (PII), including full name, social security number, driver's license number, home or work address,

birthday, credit card number, or any information that may harm AACPS and its stakeholders, if disclosed.

5. ***Telecommunications* –** the entire technological infrastructure that handles voice, video, and data traffic that either begins, ends, or continues within AACPS property.

6. ***Technology* –** hardware or software, including computers, laptops, servers, tablets, switches, routers, firewalls, wireless devices, telephones, cellular phones, audio equipment, video equipment, software systems, online resources, and email.

7. ***User or Users* –** AACPS employees, students, parents/guardians, organizations, or approved third parties accessing or utilizing school system technology or telecommunication services.

D. PROCEDURES

1. Acquisition of Technology

a. The purchase of technology shall be in accordance with Policy DEC – Vendor Relations.

b. Technology donations shall be in accordance with Policy DCA – Gifts, Bequests, Donations, and Solicitations.

c. Technology grants shall be in accordance with Policy DJ – Grants, Mini-Grants, and Special Projects.

2. Acceptable Use of Technology

a. Users may only use AACPS technology:

i. In a civil, ethical, legal, and responsible manner in accordance with AACPS policies, regulations, and State law.

ii. To communicate with their elected representatives only for AACPS educational purposes.

b. Users may not use AACPS technology:

i. For commercial purposes, defined as offering or providing goods or services for personal use;

ii. For personal lobbying or other personal political activities;

iii. To gain or attempt to gain unauthorized access to any technology or data. This is strictly prohibited and constitutes a violation of this regulation and its accompanying policy;

iv. To knowingly deploy malware or other software with malicious intent;

v. To eavesdrop on AACPS telecommunications or related services;

vi. To access AACPS-provided technology via another individual user's account credentials, except in emergencies. After emergency access has been granted, the account credentials that were used shall be changed as soon as possible;

vii. To attempt to circumvent, modify, or disable technology security protection measures implemented by AACPS, including:

a) Anti-malware software;

b) Internet content filter;

c) Network and system policies;

d) Network firewalls;

e) Intrusion detection and prevention systems; and

f) Computer and server administrative management software;

viii. To engage or participate in any illegal act such as arranging for the purchase of drugs, alcohol, or other controlled substances, engaging in criminal activity, threatening the safety of any person, or participating in any activity that may be improper, illegal, unethical, or inappropriate;

ix. To access, write, store, or publish material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people;

x. To communicate obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language, pictures, or gestures;

xi. To engage in personal attacks, including the writing or posting of any defamatory, prejudicial, or discriminatory media;

xii. To make statements that are libelous, defamatory, slanderous, or that harass another person;

xiii. To copy or transfer copyrighted materials and software without proper authorization;

xiv. To store or execute games or personal software applications without prior approval from the Chief Information Officer or the Chief Information Officer's designee; or

xv. To stream audio or video from the Internet for unauthorized personal use such as listening to Internet radio stations or streaming video.

c. Users shall:

i. Promptly disclose to appropriate school system personnel any communication or materials that are or may be inappropriate or that makes them feel uncomfortable;

ii. Comply with requests from appropriate school system employees to cease activities that threaten the operation or integrity of any AACPS technology component;

iii. Alert the school principal or principal's designee and the Chief Information Officer or the Chief Information Officer's designee if they are aware of suspicious or inappropriate use of AACPS technology, including abuse and possible breaches of security;

iv. Take reasonable precautions to protect AACPS-issued technology and related data against damage, theft, loss, or disclosure; and

v. Be financially responsible for costs incurred due to an individual's negligence or misuse that result in the destruction, loss, or theft of AACPS technology.

d. Users may not damage, destroy, or tamper with the integrity of electronic information, data, or content.

e. Users may not make unauthorized copies or reproductions of AACPS information or data.

f. Failure by any user to comply with this regulation and accompanying policy may result in the temporary or permanent suspension of technology access privileges, in addition to any applicable legal action, disciplinary action, or financial obligation.

g. Employees may, on a limited and infrequent basis only, use AACPS technology for personal use. Except in emergency situations, employees shall limit personal use of AACPS technology to lunch breaks and scheduled work breaks only. Such

usage may not affect an employee's productivity and if it does, it shall cease immediately. An employee's supervisor is authorized to determine whether such usage is affecting the employee's productivity. In such cases, besides disciplinary action, the employee's personal use may be suspended or revoked. Employees shall avoid using AACPS technology for personal use during otherwise productive business hours. In addition to the other conditions described in this regulation, employees are specifically prohibited from using AACPS technology to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, participate in organized labor activities or union business, except as permitted under State or federal laws or the applicable Negotiated Agreement, or promote or solicit funds for a religious or other personal cause. During periods of anticipated high or mission critical activity, AACPS may restrict or prohibit personal use in order to preserve resources for business use.

3. **Data Privacy**

   a. Content transmitted using AACPS technology is subject to relevant Board of Education of Anne Arundel County (Board) policies.

   b. AACPS technology users shall comply with all applicable federal, State, and local laws and regulations, including:

      i. The Family Educational Rights and Privacy Act;

      ii. The Children's Online Privacy Protection Act;

      iii. The Protection of Pupil Rights Amendment; and

      iv. The Maryland Student Privacy Act of 2015.

   c. AACPS technology users shall have no expectation of privacy in the contents of their electronic files on any AACPS-provided systems and storage devices.

   d. Users shall password protect electronic files containing sensitive information.

   e. AACPS reserves the right to access or disclose, for investigative purposes, the contents of electronic communications, files, and other materials created, stored, or accessed using AACPS technology.

   f. AACPS reserves the right to archive, audit, or purge the contents of electronic communications, files, and other materials created, stored, or accessed using AACPS technology.

g. Electronic files created or stored on AACPS-provided technology belong to AACPS. Therefore, accessing such files by AACPS authorized personnel is not considered surveillance and privacy laws do not apply.

h. Routine maintenance and monitoring of the network or audits may lead to the discovery that a user has or is violating the law, Board policy, or AACPS regulation. If this occurs, an investigation into the violation may be conducted.

i. An individual search of technology and related data shall be conducted if determined necessary or appropriate by the Division of Investigations, the Chief Information Officer, or the Division of Safe and Orderly Schools.

j. Electronic files stored on AACPS technology may be available under State public information or records laws and may be discoverable in litigation or disclosable under the Public Information Act. Information written or transmitted using AACPS technology may be read or viewed by any properly authorized individual, organization, or agency.

k. Employees may not disclose student data, employee data, or other AACPS-owned data to any third party unless directed to do so by their immediate supervisor or administrator.

l. Vendor contracts shall include appropriate non-disclosure agreements for the protection of AACPS data and their stakeholders.

m. AACPS electronic data shall be physically stored within the United States to ensure that all United States data privacy and protection laws and regulations are applicable. Exceptions may be made only with prior approval from the Superintendent or the Superintendent's designee.

4. **Protection of AACPS Technology and Related Data**

a. AACPS reserves the right to take any and all necessary actions to protect the availability, confidentiality, and integrity of its technology and related data.

b. AACPS reserves the right to take any and all necessary actions to prevent its technology from being used to attack, damage, harm, or exploit others.

5. **Electronic Communications**

a. Electronic communications created, received, or stored on AACPS electronic communications systems are the sole property of AACPS and not the author, recipient, or user.

b. Users shall have no expectation of privacy or confidentiality of any electronic communication using AACPS electronic communications systems.

c. Electronic communication of sensitive data shall be encrypted to ensure the confidentiality of the data being transmitted. Users shall ensure that websites to which they are transmitting sensitive data contain the URL header of https:// rather than http:// to ensure the confidentiality of the data being transmitted.

d. Users may not use AACPS electronic communications systems for personal, commercial, profitable, religious, or political use.

e. Users may not use AACPS electronic communications systems to transmit messages, images, cartoons, epithets, or slurs based upon actual or perceived race, ethnicity, color, religion, national origin, sex, age, marital status, sexual orientation, genetic information, gender identity, gender expression, disability, or homeless status.

f. AACPS systems that store or transmit sensitive employee data, student record data, financial data, or other legally confidential data shall implement appropriate authentication technologies to prevent unauthorized access or modification.

g. Users of AACPS electronic communications systems shall ensure that both their usage and electronic communications content are in compliance with all other AACPS policies and regulations and applicable negotiated agreements.

h. Users may not post or send via email chain letters or other unsolicited messages, also known as sending spam. Spam distribution using AACPS technology is strictly prohibited.

i. Broadcast emails, or messages to a large number of individuals or groups through the network, shall be administrative, educational, or instructionally related. Solicitation emails for fundraisers or other non-educational events are considered spam.

j. Users may not transmit user account credentials to other parties using non-secure communications, including email and interoffice mail.

k. AACPS shall conduct email communications regarding AACPS matters on AACPS-approved email systems.

6. **Physical and Environmental Security**

a. Physical access to data centers, main distribution frames, and intermediate distribution frames shall be controlled to restrict, prevent, and detect unauthorized access to these areas. Access to these areas shall only be provided to individuals

who have legitimate responsibilities for these areas and the contents contained in these areas.

b. Data centers shall be secured using technologies that monitor individual access and provide non-reputable access logs for investigative purposes.

c. Individuals and users shall take reasonable steps to ensure the physical security of AACPS technology and data.

d. Users shall log out, lock, or shutdown computers when unattended. Exceptions shall be made for computer labs and public access computers and kiosks.

e. AACPS may employ technologies that log out, lock, or shutdown computers after pre-defined periods of inactivity.

7. **Asset Management**

a. Applicable technologies shall be accounted for and tracked by serial number, asset tag number, assignment location, and owner.

b. Technology equipment, software, and peripherals may not be removed from schools without express written authorization from the Chief Information Officer or the Chief Information Officer's designee.

c. The physical removal of technology equipment from AACPS property shall be done in accordance with policies and procedures set forth by the Division of Facilities. Any sensitive data residing on this equipment shall be removed in compliance with the current National Institute of Standards and Technology published standards.

d. AACPS technology equipment shall be disposed of in accordance with the current National Institute of Standards and Technology published standards.

8. **Access Control**

a. The Chief Human Resources Officer shall notify the Office of Information Technology through established protocols when a change in employment status for an employee occurs.

b. The Superintendent or the Superintendent's designee shall modify user account privileges based on changes to employment status.

c. The Chief Information Officer or Chief Information Officer's designee shall receive automated notification from the student information system when a

student is enrolled in AACPS or if the student information or enrollment status has changed.

d. The Superintendent or the Superintendent's designee shall modify student user account privileges based on changes to enrollment status.

e. The Chief Information Officer or the Chief Information Officer's designee shall maintain a process for the creation, modification, and disabling of contractor, guest, and temporary user account privileges.

9. **User Credential Assignment and Use**

a. AACPS employees shall be assigned individual account credentials once they are employed with AACPS.

b. Students shall be assigned individual account credentials once they are enrolled in AACPS. Generic accounts may be used for primary grades, as needed.

c. Contractors, volunteers, interns, and others shall be assigned individual account credentials after approval has been granted by the Superintendent or the Superintendent's designee.

d. Users of AACPS technology shall authenticate using their unique assigned account credentials, when applicable.

e. Users are responsible for the use of their individual account credentials and shall take reasonable precautions to prevent others from being able to access or use their account credentials.

f. Users shall be required to change temporary passwords upon next login.

g. Users shall change their password immediately if they suspect it has been compromised.

h. User password length and complexity requirements shall be established for each system by the Chief Information Officer or the Chief Information Officer's designee to prevent unauthorized access to or modification of confidential or private data.

i. Default user passwords shall be unique to the individual recipient.

j. In situations where individual accounts are not available, users are prohibited from sharing user account credentials, unless expressly permitted by the Chief Information Officer or the Chief Information Officer's designee.

k. Users are granted access to AACPS technology and data based on least privilege methodology.

l. Individual user account credentials may not be assigned local administrator access to computing equipment, including desktops, laptops, servers, and tablets unless approved, in writing, by the Chief Information Officer or the Chief Information Officer's designee.

m. User access to AACPS technology shall be terminated when the individual's role is fulfilled or terminated.

10. **Employee User Account Credential Guidelines**

a. Passwords may not be the same as the user ID.

b. Passwords may not be shared with others.

c. Passwords shall be a minimum of eight characters and shall meet at least three of the following four requirements:

i. Upper case letter;

ii. Lower case letter;

iii. Number; and

iv. Special character, which is highly desirable.

d. Password changes shall be required at various intervals, depending on the capabilities of the system.

e. Password reuse is strongly discouraged.

f. System and directory service passwords shall expire at a minimum of every 45 days and at a maximum of every 180 days, depending on the capabilities of the system.

g. Employee user accounts shall be disabled for 60 minutes after five consecutive unsuccessful login attempts. For systems that cannot meet this requirement, the most stringent capability shall apply.

h. Employee user accounts shall expire after 90 days of inactivity unless otherwise directed by the Superintendent or the Superintendent's designee.

i. AACPS reserves the right to modify employee account credentials for individuals upon change in employment status and directed by the Superintendent or the Superintendent's designee.

j. Employees who separate from employment shall have their accounts disabled as soon as practically possible.

k. Shared user accounts are permitted only when they are required to provide specific access or functionality or when multi-user access is not available.

11. **Student User Account Credential Guidelines**

a. Passwords may not be the same as the user ID.

b. Passwords may not be shared with others.

c. Password changes shall be required as needed.

d. AACPS reserves the right to disable student accounts.

e. Students who leave AACPS shall have their accounts disabled.

f. Password reuse is strongly discouraged.

g. Student user accounts shall be disabled for 60 minutes after five consecutive unsuccessful login attempts. For systems that cannot meet this requirement, the most stringent capability will apply.

h. Student user accounts shall expire after 180 days of inactivity unless otherwise directed by the Superintendent or the Superintendent's designee.

i. Shared user accounts are permitted only when they are required to provide specific access or functionality or when multi-user access is not available.

12. **Storage Media Security and Disposal**

a. Access to AACPS storage media, including magnetic tapes, internal and external hard drives, CDs, DVDs, and flash drives shall be secured using least privilege methodology. When applicable, encryption technologies shall be used to protect sensitive data.

b. AACPS storage media, including magnetic tapes, internal and external hard drives, CDs, DVDs, and flash drives shall be disposed of in accordance with the current National Institute of Standards and Technology publications.

13. **Telecommunications and Network Security**

    a. Users may not connect non-AACPS owned technology to any AACPS network, whether wired or wirelessly, without prior written approval by the Chief Information Officer or the Chief Information Officer's designee.

    b. No person may install wiring, wireless connections, or any extension or retransmission of network services without the express written approval of the Chief Information Officer or the Chief Information Officer's designee.

    c. Users may not scan the network to examine or determine security or monitoring measures.

    d. Users shall follow guidelines concerning use of telecommunication connections, networks, and applications as established by the Office of Information Technology and published in the AACPS *Employee Handbook,* AACPS *Student Handbook*, Board policies, and AACPS regulations.

    e. Wireless access points shall be configured utilizing Wi-Fi Protected Access 2 (WPA2) or greater encryption for transmissions, unless an exception has been expressly approved by the Chief Information Officer or the Chief Information Officer's designee.

14. **Software and Database Security**

    a. ***Systems Development Life Cycle***

        i. AACPS applications and systems shall be developed or procured in compliance with all local, State, and federal laws and regulations.

        ii. When administratively appropriate, all AACPS applications shall employ the latest software versions and patch levels to ensure maximum functionality and security.

        iii. AACPS training system data may not include confidential information.

        iv. AACPS application and source code shall be managed in a secure, controlled, and auditable environment.

    b. ***Software Licensing***

        i. Software and systems shall comply with applicable vendor licensing and fair use agreements. Users shall abide by the vendor Terms of Service and privacy policy.

ii. Software and systems that do not publish Terms of Service and a privacy policy may not be used for AACPS-sanctioned activities.

iii. Free and open-source software shall be approved prior to use by the Chief Information Officer or the Chief Information Officer's designee.

15. **Security Operations**

a. The Chief Information Officer or the Chief Information Officer's designee is authorized to monitor AACPS technology for potential misuse and security violations.

b. The Chief Information Officer or Chief Information Officer's designee shall coordinate annual technology security vulnerability assessments and penetration tests in accordance with current industry best practices.

c. AACPS may contract with third party individuals or organizations to perform vulnerability assessments and penetration tests.

d. AACPS may employ encryption technologies for hard drives, flash drives, databases, and other storage media, as necessary, to further secure sensitive AACPS technology-related data.

16. **Security Investigations – Students**

Investigations that lead to search and seizures on school property involving technology shall be in accordance with State law and regulations and Regulation JCC-RAJ – Search and Seizure.

17. **Policy and Regulatory Compliance**

a. In accordance with the Children's Internet Protection Act, AACPS shall deploy technologies which attempt to filter abusive, libelous, obscene, offensive, pornographic, illegal, or otherwise inappropriate material.

b. AACPS-sponsored online systems shall comply with the Children's Online Privacy Protection Act.

c. AACPS is not responsible for, nor does it control, information and content found on outside networks including the Internet.

18. **Disclaimer of Liability**

a. AACPS cannot guarantee the availability of or access to the Internet and other telecommunication services. AACPS may not be responsible for any information

or data that may be lost, damaged, or become unavailable due to technical, hardware, software, or power difficulties and failures.

b. AACPS cannot guarantee the accuracy and quality of information acquired via any component of AACPS technology infrastructure.

c. AACPS provides no assurance or guarantee that information, email, or any other communications transmitted via the network is or will remain private and confidential.

d. Even though the network uses blocking and restriction devices or services, the school system cannot guarantee comprehensive control of, or censor, illegal, defamatory, inaccurate, obscene, or potentially offensive materials that may be transmitted via the Internet or through the network.

19. **Incident Response**

a. The Division of Investigations, the Office of Information Technology, and Division of Safe and Orderly Schools reserves the right to access, intercept, and record electronic communications, files, and other data for investigative purposes.

b. AACPS shall maintain technology security incident response procedures in support of this policy and regulation.

c. Technology security investigations shall be confidential.

d. The results of any investigations shall be shared with those who need to know for appropriate handling and resolution.

e. AACPS technology security investigations shall be authorized, in writing, by the Superintendent or the Superintendent's designee.

f. AACPS shall document AACPS technology security incidents and investigations.

g. AACPS reserves the right to access, record or, if necessary, remove content stored in an individual's assigned account or storage location with prior written approval from the Superintendent or the Superintendent's designee.

h. AACPS reserves the right to restrict or remove access to any device suspected of contributing to a security incident.

20. Dissemination of this Policy and Regulation

The Chief Information Officer or the Chief Information Officer's designee shall communicate the provisions of this policy and regulation annually or, as needed, through customary mechanisms.

21. Policy and Regulatory Violations

a. An individual who suspects a violation of this regulation or accompanying policy shall report the alleged violation to an appropriate administrator, the Chief Information Officer, or the Division of Investigations.

b. An administrator or supervisor shall report the suspected violation to the Division of Investigations, Division of Safe and Orderly Schools, or Chief Information Officer, as appropriate.

c. The Division of Investigations or the Division of Safe and Orderly Schools shall follow through on a report of a suspected violation for an appropriate resolution.

Regulation History: Issued 04/06/16; Revised 04/17/19; 11/20/24

Note Previous Regulation History: None

Legal References: Family Educational Rights and Privacy Act; 34 C.F.R. Part 99; Children's Online Privacy Protection Act; 16 C.F.R. §312, et seq.; Protection of Pupil Rights Amendment; 34 C.F.R. §98.1 et seq.; Maryland Public Information Act; Section 4-131 of the Education Article; COMAR 13A.08