

---

I. Policy: 409

II. Procedure:

A. *Scope -- These procedures apply to all school system information systems facilities and communication networks, and to the information stored and processed on these facilities.*

1. Intent:

- a. *Ensure the confidentiality, availability, and integrity of data;*
- b. *Reduce the risk of data loss by accidental or intentional modification, disclosure, or destruction;*
- c/ *Preserve the school system's rights and remedies in the event of such a loss.*

2. *School system data consists of confidential as well as uncontrolled documents and other information considered to be critical to the missions of individual departments and the school system as a whole. Access to information is on a "need to know" basis only.*

3. *Each individual using school system property is responsible for understanding the data security procedure and complying with its terms.*

4. *All school system information shall be protected against theft, malicious damage, unauthorized access, tampering, and loss.*

5. *All school system computer systems shall include controls which ensure that the appropriate privacy and confidentiality of data are maintained and that data accuracy and integrity are preserved throughout the life of the application.*

---

State Law: *Educ. Art. §§4-101, 4-107; Art. 27, §146*

State Reg.: *COMAR 13A.08.02.03*

Federal Law: *Family Educational Rights and Privacy Act (FERPA)*

Adm. Reg.

Neg. Agr.:

Other Citation:

6. *All systems, including instructional applications, shall implement backup and contingency plans to ensure that operations or functions may be continued if any equipment or personnel become unavailable.*
  7. *Users accessing any sensitive school system information will be required to submit sufficient identification and authentication to ensure that they have access only to the data they are authorized to use.*
    - a. *Each user will be responsible for ensuring the confidentiality of his/her identification and authentication.*
  8. *Communications must be undertaken only over dedicated lines. Other communication facilities (e.g., dial-up) will be considered only if an appropriate level of protection can be ensured.*
- B. Personnel -- All persons with access to the school system's informational resources must review and understand these security procedures. Personnel procedures should be in place to address the following items:*
1. *Procedures after Termination and Transfer: Whether initiated by the employee or the organization, termination and transfers can present unique security threats to information resources. Procedures should be developed and responsibilities assigned to specific departments in an organization to address the following:*
    - a. *Cancellation of access privileges to critical areas, to specific data systems, and to the installation as a whole;*
    - b. *Return of school system property, i.e., keys, photo-ID badges, passes, magnetic storage media, and passwords for supervisory access User IDs;*
    - c. *Notification to the Information Security Administrator via the Help Desk, of the change in employee status (especially procedures for discontinuing passwords). Notification by employee's supervisor to the Help Desk will be given an Urgent designation.*

2. *Contract Employee Access: Access may be restricted to specific terminal locations and granted for a period of days, weeks, or months, and should automatically expire at the end of the period. Access should be restricted to specific information systems data or resources.*
  3. *Interagency Connectivity: County Government and Community College connectivity refers to the sharing or granting of access between separate organizations; information systems data or resources. Access to information systems resources by this group is subject to the same “need to know” discretion as employees of AACPS.*
  4. *School Volunteers: School volunteers, parents, community members, business partners, etc., all must undergo training programs specifically tailored to non-employee status individuals and their potential access to sensitive data. Access to information systems resources by this group is subject to the same “need to know” discretion as employees of AACPS.*
  5. *Students: Students must comply with all applicable Board Policies, Administrative Regulations, and school rules.*
- C. *Operational Procedures -- Operational Procedures define the day-to-day controls necessary to protect operational application systems. This section outlines specific measures which must be taken and the circumstances under which those security measures must be considered.*
1. *Physical Security: All school system computer equipment, software, documentation, and storage media shall be protected against theft, damage, unauthorized access or tampering, and environmental hazards.*
  2. *Safety: The Department of Technology and Information Services is responsible for developing technical specifications that will operate in a safe manner. Only Department of Technology and Information Services, authorized maintenance vendors and designated personnel trained by Technology and Information Services are allowed to physically modify computer equipment.*

*All diagnostic, maintenance, and system unit enhancement work will follow vendor-prescribed safety procedures and generally accepted electronic and electrical equipment safety standards.*

*The Facilities Planning and/or Maintenance Department will ensure that all appropriate codes are adhered to in the construction of a computer lab.*

3. *Location Planning: All requests for new or relocated equipment must come to Technology and Information Services and where applicable, the Department of Instruction, and be accompanied by a sketch of the proposed location.*
4. *Facilities Modification: The requesting department must contact the Department of Technology and Information Services and where applicable, the Department of Instruction, to ensure that the furniture and storage facilities are sufficient before the planned installation date. If electrical or temperature control modifications are required, a Major/Minor Work Request must be submitted to Maintenance.*
5. *Relocation Within a Department: The Telecommunication Section of the Department of Technology and Information Services maintains an inventory of equipment and other detailed records including LAN configuration data critical to the operation of the network.*
  - a. *Network Equipment: Relocation involving equipment that is connected to other equipment through telecommunication cables or equipment must be coordinated with the Department of Technology and Information Services.*

*The department in charge of the equipment should submit a work request as early as possible in the planning stage of a relocation. Floor plans or sketches are required and should be attached to request.*
  - b. *Stand Alone Equipment: The relocation of stand-alone workstations, (including docking stations) that are not networked can be accomplished by the responsible*

*department without prior notification of the Department of Technology and Information Services. This applies only to equipment with cables which can be contained entirely within a cubicle or furniture workstation.*

- c. Portable Equipment: Computer equipment which is specifically designed and intended to be used in multiple locations is exempt from relocation procedures.*
- d. Software: The requesting department is responsible for providing the Department of Technology and Information Services with a list of items pertinent to the transfer, including the specific software (uniquely identified in some manner, e.g., by serial number), new location, new department, and date relocation is desired.*

*The Department of Technology and Information Services is responsible for all administrative software. This software includes all application programs and operating system software developed or acquired by the Department of Technology and Information Services.*

- 6. Environmental Protection: Computers and their related equipment are sensitive to dust, smoke, and dirt. It is the responsible department's obligation to make sure the equipment and area are kept clean.*
- 7. Electrical Conditioning and Backup Power: Technology and Information Services and Facilities Management will address electrical conditioning and backup power supplies in the planning phase of all projects that involve the installation of computer equipment.*
- 8. Temperature and Humidity: It is the duty of the responsible department or school to notify the Operations Division when the temperature and humidity guidelines specified by the manufacturer, are not being met. Refer to the operations literature supplied with the equipment for specific equipment guidelines.*

9. *Equipment Removal: The physical removal of computer equipment from school system premises must be done in accordance with policies and procedures set forth by the Property Control Department. Any school system property residing on this equipment including information, hardware, or software must be removed in compliance with appropriate local, state, and federal laws. This includes equipment on loan to the school system as well as the personal property used by employees, volunteers, students, and contractors.*

10. *Maintenance and Modification: Maintenance and modification of computer equipment shall be coordinated by the Department of Technology and Information Services.*

*Computer equipment is not to be physically modified without the express authorization of the Department of Technology and Information Services. Only the Department of Technology and Information Services, authorized service providers and designated personnel trained by Technology and Information Services are allowed to physically modify computer equipment. Physical modification does not cover the disconnection of equipment components for relocation purposes.*

11. *Use of Non-School System Property: Any equipment which is not the property of the school system but will come into contact with school system information systems is subject to the same policies and procedures governing school system property. This includes equipment on loan to the school system as well as the personal property used by employees, volunteers, students, and contractors.*

D. *Communications --*

1. *Adequate security must be maintained when using facilities that access data among terminals and computers over telecommunications networks.*

2. *Communication with any school system computer or computer networks, including but not limited to mainframes, minicomputers, local area networks, or stand alone PCs, must be accomplished using approved data security techniques.*

3. *The Department of Technology and Information Services, in consultation with members of the Auditing Department, is responsible for the security of all computer communications and maintaining audit trails for communications.*
4. *Requests to add or alter external communication links attached to school system computer equipment must be approved by the requesting department's manager and then forwarded to the Director of Technology and Information Services for evaluation and approval. The Information System Security Administrator and telecommunications personnel will review the request and recommend the appropriate course of action.*
5. *Three types of access have been identified, each of which will require some combination of administrative as well as technological control. In each case, when permission is granted, the approval will be only for a specifically approved purpose. Any new application requires a new request for approval.*
  - a. *Dial-Out Only: This describes unrestricted dial-out access initiated within a school or office. The computing devices having modems attached may include PCs attached to LANs or PCs with mainframe links only if specific approved equipment (e.g., security modems) and procedures are used and followed. Access approvals will be maintained by Technology and Information Services Security. Additions to the list can be requested by users on an as-needed basis. For Dial-Out applications to other school system computing facilities, a department must maintain an inventory of users and their specific applications.*
  - b. *Positive Voice Identification Dial-In: Dial-in to any school system computing device allows access for specific individuals that have been identified and authorized for access after positive voice identification has been established for each access. Dial-in users must submit request forms for approval to Technology and Information Services Security, and a log of these requests must be kept.*

- c. *Technological Dial-In: Dial-in users must submit request forms for approval to Technology and Information Services Security, and a log of these requests must be maintained. These applications will require case by case technical and procedural analyses and resolutions (e.g., card-key access control, encryption, etc.).*
  - d. *Internet: Use of the Internet is limited to outgoing connections only with the exception of E-Mail and restricted desk top video teleconferencing. Leased line access must have adequate firewall software installed to filter all incoming traffic. No Internet Protocol addresses should be permitted as incoming traffic.*
  - e. *Student Use of the Internet or Other on-line Services will be supervised by adults and/or monitored via firewall software. The goal is to prevent student access to undesirable (pornographic, etc.) materials.*
  - f. *Usable software downloaded from Internet bulletin boards must first undergo virus detection and removal. Its use is restricted according to Federal Copyright Law.*
- E. *User Awareness -- User awareness is an essential component of an effective security program. The purpose of a security awareness program is to inform personnel of the importance of the information they handle and the legal and business reasons for maintaining its integrity, confidentiality, and availability. User awareness programs are:*
- 1. *Training: Programs that elevate employee's awareness of information as an asset are necessary to ensure that information is adequately protected. All employees, as well as parents and volunteers, must be trained in proper computer ethics, virus control, and legal issues related to the use of our informational resources.*
  - 2. *Maintaining Security Awareness: All training tends to be forgotten over time. Consequently, the security awareness program must be ongoing to remind employees of their role and responsibilities in the total security program.*

3. *General Reminders: Notices or posters reminding employees of security requirements are to be placed in areas where sensitive information is handled.*
4. *Publications: General security measures affecting all computer users will be published in booklets distributed by Anne Arundel County Public Schools. Examples of such publications are the Employee Handbook and Making the Home/School Connection.*