REGULATION ANNE ARUNDEL COUNTY PUBLIC SCHOOLS

Related Entries: DL, DI, DI-RA, IH, IH-RA
Responsible Office: DIVISION OF TECHNOLOGY

DATA GOVERNANCE

A. PURPOSE

To establish procedures for the management and maintenance of data privacy and security practices in the processing of personally identifiable information across the Anne Arundel County Public Schools (AACPS) information technology and records management systems.

B. BACKGROUND

In accordance with State law, AACPS commits to implementing best practices on data governance and professional development on data governance policies and procedures.

The Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) govern the privacy of student data when educational institutions engage cloud service providers. FERPA generally prohibits disclosure, by schools that receive federal education funding, of personally identifiable information from a student's education records unless the educational institution has obtained signed and dated written consent from a parent/guardian or eligible student or one of FERPA's exceptions applies. COPPA governs operators of websites and online services that are directed to children younger than age 13 and operators of general audience websites or online services that have actual knowledge that a user is younger than age 13.

C. DEFINITIONS

1. ***Data Owner*** – an individual who has the requisite knowledge, administrative control, and has been officially designated as accountable for specific data elements or data sets.

2. ***Data Steward*** – an individual who is responsible for maintaining data quality and security.

3. ***Education Records*** – those records that are directly related to a student and maintained by AACPS or by a party acting for AACPS.

4. ***Personally Identifiable Information*** – information that, alone or in combination, makes it possible to identify an individual student with reasonable certainty.

D. PROCEDURES

AACPS shall continuously improve the availability, integrity, and security of data systems through the development and enforcement of laws, policies and regulations. Accordingly, data privacy protection of AACPS technology, related data, and electronic communications shall be in accordance with Policy DI and Regulation DI-RA – Technology Use and Security.

1. AACPS shall have a data privacy and security incident response plan.

2. AACPS shall have a security breach notification plan.

3. AACPS shall maintain cyber security incident response guidelines and data breach notification procedures.

4. AACPS shall:

    a. Create and implement a data classification plan for all AACPS data to determine data sensitivity levels.

    b. Establish and maintain security controls to be implemented, in accordance with the classification plan, for each identified data security level.

5. The Superintendent or the Chief Information Officer shall identify and assign data owners and data stewards who shall oversee the collection, use, sharing, and destruction of data.

6. AACPS shall establish procedures and requirements for allowing access to student data and personally identifiable information (PII) for a legitimate research purpose. Electronic resources containing student PII may only be approved for use in accordance with the following data privacy guidelines.

    a. Communications between the client software, including web browsers, file uploads, file downloads, and the system and data at rest shall be encrypted using current *Federal Information Processing Standard 140-2* or another AACPS-approved equivalent standard to ensure confidentiality, integrity, and availability of AACPS-owned data.

    b. Cloud-hosted system providers shall warrant that the resource it will provide to AACPS is fully compliant with the following laws and regulations, if applicable:

        i. Children’s Online Privacy Protection Act;

ii. Family Educational Rights and Privacy Act;

iii. Health Insurance Portability and Accountability Act; and

iv. Maryland Student Date Privacy Act of 2015.

c. Cloud-hosted systems must adhere to *National Institute of Standards and Technology SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing*.

7. Instructional digital resources containing PII shall be reviewed and approved in accordance with Policy IH and Regulation IH-RA – Materials of Instruction – Review, Evaluation, and Selection.

8. Prior to use, non-instructional digital resources containing PII must be reviewed and approved by the Chief Information Officer or the Chief Information Officer's designee in accordance with the procedures established in this regulation.

9. AACPS shall notify students and parents/guardians annually of their rights under FERPA.

10. AACPS employees who access and maintain FERPA-protected data shall complete appropriate FERPA training annually.

11. AACPS shall follow best practices as established by the Maryland State Department of Education to ensure transparency in data sharing with third parties.

Regulation History: Issued 04/21/21

Note Previous Regulation History: None

Legal References: 20 U.S.C. § 1232g; 34 CFR Part 99; Children's Online Privacy and Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act (HIPAA); Student Data Privacy Act of 2015, Sections 1-101 and 7-2101 through 7-2105 of the Education Article