Data Security and Governance

Statement of Purpose

Per the US Department of Education, "Increased demand for high-quality data and the resulting growth in the amount of individual student data collected and stored electronically by educational agencies has necessitated greater scrutiny of data management and protection practice."

Definitions

Protected Data/Information – Information that the Albemarle County Public Schools ("School Division") is prohibited by law, policy, or contract from disclosing or that the School Division may disclose only in limited circumstances. Protected data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information – Information that is determined to be essential to School Division operations and that must be accurately and securely maintained to avoid disruption to School Division operations. Data relates to original or authoritative content and may reside on different and multiple physical medias.

Data Governance – Following best practice guidelines for ensuring that an organization's data and information assets are managed consistently and used properly.

Personally Identifiable Information (PII) - is information that, when used alone or with other relevant data, can identify an individual.

Scope

The Superintendent is authorized to establish, implement, and maintain data and information security measures. The policy, standards, processes, and procedures apply to all students and employees of the School Division, contractual third parties and agents of the School Division, and volunteers who have access to School Division data systems or data.

Regulatory Compliance

The School Division will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. The School Division complies with all applicable regulatory acts including, but not limited to the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)

- Virginia Public Records Act
- Individuals with Disabilities in Education Act (IDEA)

Responsibility and Data Stewardship
All School Division employees, volunteers and agents are responsible for accurately collecting, maintaining, and securing School Division data including, but not limited to, information that is protected or is critical to School Division operations. The School Division will maintain a documented Incident Response Plan if a data security breach occurs and will follow the required reporting structures.

Data Managers
Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. All administrators of the School Division, including, but not limited to, Assistant Superintendents, Principals, Directors, and their designees are data managers for all data collected, maintained, used, and disseminated under their supervision as well as data they have been assigned to manage. Data managers will monitor access to the information to ensure that protected information is accessed only by individuals who need the information to provide services to the School Division and that protected and critical information is modified only by authorized individuals.

Data managers will:

- assist in enforcing School Division policies and procedures regarding data management.
- ensure that system account creation and associated data access match staff member job function within all systems.
- approve all staff with custom data access beyond their typical group's access.
- ensure that data will be maintained accurately.
- review contracts with instructional and operational software providers to ensure that they are current and meet the School Division's data security guidelines, by following the ACPS application/system vetting process.
- ensure that staff are trained in the School Division's proper procedure and practices in order to ensure accuracy and security of data.
- assist the Superintendent/designee in enforcing School Division policies and procedures regarding data management.

Protected and Critical Information
The School Division will collect, create, or store protected information only when the Superintendent/designee determines it is necessary. The School Division will provide access to protected information to appropriate employees and volunteers only when the School Division determines that such access is necessary for the performance of their duties.

All School Division staff, volunteers, contractors, and agents who are granted access to critical and protected information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of protected information. All individuals using protected and critical information will strictly observe protections put into place by the School Division including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of

password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

School Division employees, contractors, and agents will notify the Chief Technology Officer ("CTO")/designee immediately if there is reason to believe protected information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise.

Securing Data at Rest and In Transit
School Division data security applies to all forms of data, including data stored on devices, data in transit, and data stored on additional resources. Regular transmission of student data to internal and external services is managed by the Department of Technology using a secure data transfer protocol. Digital transmission of protected student records to external entities must be transferred via a secure method.

NOTE: Anyone issued a School Division laptop must obtain approval from the Chief Technology Officer/designee before taking a School Division-owned laptop out of the country because traveling internationally can pose significant risks to information stored on or accessible through laptops.

Using Online Services and Applications
School Division staff members are encouraged to research and utilize online services or applications to engage students and further the School Division's education mission. However, before any online service or application is purchased or used to collect or store protected or critical information, including directory information regarding students or employees, the CTO/designee must approve the use of the service or application and verify that it meets the requirements of the law and Albemarle County School Board Policies and appropriately protects protected and critical information. This prior approval is also required when the services are obtained without charge.

New Digital Resources and Systems
The School Division has established a process for vetting new digital resources and systems. Staff are required to complete the process in order to ensure that all new resources meet business and/or instructional needs as well as security requirements.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Alignment with curriculum and instruction goals
- Account provisioning structure and responsibility
- Support and resources for professional development and/or training
- Duplication of services or features in existing resources
- Impact on technology environment, including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements, including cost
- Resource update and maintenance schedule
- Resource meets security guidelines

- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract following the ACPS vetting process

A current list of all vetted and approved software systems, tools and applications is published on the School Division's website. It is the responsibility of staff to submit a request to use a new digital resource if a resource is not listed.

Training
The CTO/designee will provide appropriate training to employees who have access to protected or critical information to prevent unauthorized disclosures or breaches in security. School Division employees will receive annual training in the confidentiality of student records.

Data Retention and Deletion
The School Division shall establish appropriate safeguards, policies, procedures, and practices for each phase of the data lifecycle. The CTO/designee shall establish a retention schedule for the regular archiving and deletion of data stored on School Division technology resources, including E-mail. The retention schedule must comply with the Library of Virginia records retention guidelines.

Employees are personally responsible for the records they create, including e-mails received and sent as well as any attachments. Individuals should be aware that the Division follows the Library of Virginia retention schedules and that all emails generated from a Division account are subject to the Freedom of Information Act.

Litigation Hold
In the case of pending or threatened litigation or when litigation is reasonably anticipated, the School Board Attorney will issue a litigation hold directive to the Superintendent/designee and other School Division employees as necessary. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by the School Board Attorney. E-mail and other technology accounts of separated employees that have been placed on a litigation hold will be maintained by the Department of Technology until the hold is released. No employee who has been notified of a litigation hold may alter or delete any electronic record that falls within the scope of the hold. Violation of the litigation hold may subject an employee to disciplinary action.

Cross References:

Federal	Description
15 U.S.C. § 7001-7006	Electronic Signatures In Global And National Commerce Act
15 U.S.C. §§ 6501-6506	The Children's Online Privacy Protection Act
20 U.S.C. § 1232g	Family Educational Rights and Privacy Act
20 U.S.C. § 1232h	Protection of Pupil Rights Amendment

Federal	Description
20 U.S.C. § 1400-1417	Individuals with Disabilities Education Act
20 U.S.C. § 7926	Elementary and Secondary Education Act
29 C.F.R. § 1630.14	Federal Regulation

State

§ 18.2-186.6.	Breach of personal information notification.

County

AP-3	Use of Technology
AP-3.1	Guidelines when Traveling Abroad

ACPS Policy References:

GDA/IIBE, Acceptable Use of Technology

JO, Student Records

JRCA, School-Service Providers' Use of Student Personal Information