3.52 - Data Governance and Use

3.52

DATA GOVERNANCE AND USE **3.52**

1. It is the policy of Alexander City Schools that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.

1. The data governance policies and procedures are documented and reviewed annually by the Data Governance Committee.

1. Alexander City Schools conducts annual training on their data governance policy and documents that training.

1. The term data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

1. **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 district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data.

This policy applies to all forms of Alexander City Schools' data and information, including but not limited to:

1. Speech, spoken face to face, or communicated by phone or any current and future technologies;

1. Hard copy data, printed or written;

1. Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.;

1. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc.;

1. Data stored on any type of internal, external, or removable media or cloud based services.

III. REGULATORY COMPLIANCE

The district shall abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Alexander City Schools complies with all applicable regulatory acts including but not limited to the following:

1. Children's Internet Protection Act (CIPA)
2. Children's Online Privacy Protection Act (COPPA)
3. Family Educational Rights and Privacy Act (FERPA)

4. Health Insurance Portability and Accountability Act (HIPAA)
5. Protection of Pupil Rights Amendment (PPRA)

1. **RISK MANAGEMENT**

1. A thorough risk analysis of all Alexander City Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO, or Technology Director. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level.

1. The Superintendent or designee administers periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures are implemented that mitigate the threats by reducing the amount and scope of the vulnerabilities.

1. **DATA CLASSIFICATION**

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data are classified according to the most sensitive detail they include. Data recorded in several formats (e.g., Source document, electronic record, report) has the same classification regardless of format.

1. **SYSTEMS AND INFORMATION CONTROL**

Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems. All involved systems and information are assets of Alexander City Schools shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

1. Ownership of Software**:** All computer software developed by Alexander City Schools employees or contract personnel on behalf of Alexander City Schools, licensed or purchased for Alexander City Schools use, is the property of Alexander City Schools and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

1. Software Installation and Use: All software packages that reside on technological systems within or used by Alexander City Schools shall comply with applicable licensing agreements and restrictions and shall comply with Alexander City Schools' acquisition of software procedures.

1. Virus, Malware, Spyware, Phishing and SPAM Protection: Virus checking systems approved by the District Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not turn off or disable Alexander City Schools' protection systems or install other systems.

1. Access Controls: Physical and electronic access to information systems that contain *Personally Identifiable Information* (*PII*), *Confidential information*, *Internal information* and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the Data Governance Committee and approved by Alexander City Schools. In particular, the Data Governance Committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to *PII*, Confidential information, internal information and computing resources include, but are not limited to, the following methods:

1. Authorization: Access shall be granted on a "need to know" basis and shall be authorized by the superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Director. Specifically, on a case-by-case basis, permissions may be added in to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Data Governance Committee.

Identification/Authentication**:** Unique user identification (user ID) and authentication are required for all systems that maintain or access *PII, Confidential information*, and/or *Internal Information*. Users shall be held accountable for all actions performed on the system with their *User ID*. User accounts and passwords shall NOT be shared.

3. Data Integrity: Alexander City Schools provides safeguards so that *PII, Confidential*, and *Internal Information* is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:

- Transaction audit
- Disk redundancy (RAID)
- ECC (Error Correcting Memory)
- Checksums (file integrity)
- Data encryption
- Data wipes

4. Transmission Security**:** Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. The following features are implemented:

- Integrity controls and
- Encryption, where deemed appropriate

Note: Only ACS district-supported email accounts shall be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business.

5. Remote Access: Access into Alexander City Schools' network from outside is allowed using the ACS Portal. All other network access options are strictly prohibited without explicit authorization from the Technology Director, or the Data Governance Committee. Further, *PII, Confidential Information* and/or *Internal Information* that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the Alexander City Schools' network. *PII* shall only be stored in cloud

storage if said storage has been approved by the Data Governance Committee or its designees.

6. Physical and Electronic Access and Security: Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals.

- No *PII*, *Confidential* and/or *Internal Information* shall be stored on a device itself, such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
- No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.
- It is the responsibility of the user to not leave these devises logged in, unattended, and open to unauthorized use.
-

1. Data Transfer/Exchange/Printing:

1. Electronic Mass Data Transfers: Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in accordance with this policy and be approved by the Data Governance Committee. All other mass downloads of information shall be approved by the committee and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) shall be in place when transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless the exception is approved by the Data Governance Committee.

1. Other Electronic Data Transfers and Printing: PII, Confidential Information and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible shall be de-identified before use.

1. Oral Communications: Alexander City Schools' staff shall be aware of their surroundings when discussing PII and Confidential Information. This includes, but is not limited to the use of cellular telephones in public areas. Alexander City Schools' staff shall not discuss

PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

1. Audit Controls: Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Data Governance Committee annually. Further, the committee also regularly reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews shall be documented and maintained for six (6) years.

1. Evaluation: Alexander City Schools require that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

1. IT Disaster Recovery: Controls shall ensure that Alexander City Schools can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Superintendent or Technology Director for response to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems. The IT Disaster Plan shall include the following:

1. A prioritized list of critical services, data, and contacts.
2. A process, enabling Alexander City Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. A process, enabling Alexander City Schools to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
4. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

VII. COMPLIANCE

1. The Data Governance Policy applies to all users of Alexander City Schools' information including employees, staff, students, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Alexander City Schools' procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Alexander City Schools' policies. Further, penalties associated with state and federal laws may apply.

1. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of *PII* or *Confidential Information*.
2. Unauthorized disclosure of a log-in code (User ID and password).
3. An attempt to obtain a log-in code or password that belongs to another person.
4. An attempt to use another person's log-in code or password.
5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
6. Installation or use of unlicensed software on Alexander City School technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Alexander City Schools' information, data and/or systems. This includes the unauthorized removal from ACS of technological systems, such as, but not limited to, laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain *PII* or *Confidential Information*.
8. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

Physical and Security Controls

The following physical and security controls must be adhered to:

1. Network systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

2. File servers and/or storage containing *PII, Confidential and/or Internal Information* must be installed in a secure area to prevent theft, destruction or access by unauthorized individuals.
3. Computers and other systems must be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
4. Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss. A record shall be maintained of all personnel who have authorized access.
5. Maintain a log of all visitors granted entry into secured areas of areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months. Ensure visitors are escorted by a person with authorized access to the secured area.
6. Monitor and maintain data centers' temperature and humidity levels. The American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE) recommend an inlet temperature range of 68-77 degrees and relative humidity of 40%-55%.
7. Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded should be moved without the explicit approval of the technology department.
8. Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

REFERENCE(S): **Code of Alabama**

HISTORY: **ADOPTED: NOVEMBER 18, 2014**

REVISED: DECEMBER 14, 2015

FORMERLY: NEW