Attalla City Schools

Data Governance Policy

Updated 03/15/2022

Board Approved 04/14/2022

TABLE OF CONTENTS

Resources

- ALSDE State Monitoring Checklist
- Record Disposition Requirements
- Email Guidelines
- Agreements for Contract Employees Including Long-Term Substitutes

Forms

- Student Data Confidentiality Agreement

Introduction

Protecting our students' and staffs' privacy is an important priority, and Attalla City Schools are committed to maintaining strong and meaningful privacy and security protections. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff.

The Attalla City Schools Data Governance document includes information regarding the Data Governance Committee, the actual Attalla City Schools Data and Information Governance and Use Policy, applicable Appendices, and Supplemental Resources.

The policy formally outlines how operational and instructional activity shall be carried out to ensure Attalla City Schools' data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The Attalla City Schools Data Governance Policy shall be a living document. To make the document flexible details are outlined in the Appendices. With the Board's permission, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs. All modifications will be posted on the Attalla City Schools website.

Data Governance Committee Members

The Attalla City Schools Data Governance Committee will be composed of staff representatives from each school in the district, students, parents, community members, and district leaders. The district technology director will serve as acting Information Security Officer (ISO) and Risk Manager.

Data Governance Committee Meetings

The Data Governance committee will meet annually at a minimum. Additional meetings will be called as needed.

Attalla City Schools Data Governance Policy

I. Purpose

A. It is the policy of Attalla 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.
B. The data governance policies and procedures are documented and reviewed annually by the data governance committee.
C. Attalla City Schools conducts annual training on their data governance policy and documents that training.
D. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

II. 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 Attalla City Schools' data and information, including but not limited to:

A. Speech, spoken face to face, or communicated by phone, or any current and future technologies,
B. Hard copy data printed or written,
C. Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media, etc.,
D. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc., and
E. Data stored on any type of internal, external, or removable media, or cloud based services.

III. Regulatory Compliance

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

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

See also Appendix A (Laws, Statutory, Regulatory, and Contractual Security Requirements.)

IV. Risk Management

A. A thorough risk analysis of all Attalla 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.

B. 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.

**** See also Appendix B (Information Risk Management Practices)***
**** See also Appendix C (Definitions and Responsibilities)***

V. 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) have the same classification regardless of format.

**** See also Appendix D (Data Classification Levels)***

VI. 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 Attalla City Schools and shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

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

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

****See also Appendix E (Acquisition of Software Procedures)***

C. **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 Attalla City Schools' protection systems or install other systems.

See also Appendix F (Virus, Malware, Spyware, Phishing and SPAM Protection)

D. **Access Controls:** Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential information, Internal information and computing resources are 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 Attalla 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 will 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 and/or Information Security Officer (ISO.) Specifically, on a case-by-case basis, permissions may be added in to those already held by individual users in the student information system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Data Governance Committee.

2. **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 will 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:** Attalla City Schools provides safeguards so that PII, Confidential, and Internal Information is not altered nor destroyed in an unauthorized manner. Core data is backed up to a private cloud for disaster recovery purposes. 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 which also includes 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.

    See also Resource 3: Excerpts from Email Guidelines

5. **Remote Access:** Access into Attalla City Schools' network from outside is allowed using the ACS Portals (staff, student, and parent). All other network access options are strictly prohibited without explicit authorization from the Technology Director, ISO, or 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 Attalla 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. At a minimum, staff passwords shall be changed annually.
    - 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 not to leave these devices logged in, unattended, and open to unauthorized use.

    See also Appendix G (Physical and Security Controls Procedures)
    See also Appendix H (Password Control Standards)
    See also Appendix I (Purchasing and Disposal Procedures)
    See also Appendix J (Data Access Roles and Permissions)

E. 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/or ISO 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.

   See also Appendix K (Attalla City Schools Memorandum of Agreement)

2. **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.

F. **Oral Communications:** Attalla 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. Attalla 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.

G. **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.

H. **Evaluation:** Attalla City Schools requires 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.

I. **IT Disaster Recovery:** Controls shall ensure that Attalla 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, Risk Management Officer, Technology Director, and/or ISO 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 Attalla City Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. A process enabling Attalla 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.

See also Appendix L (IT Disaster Recovery Plan)

VII. Compliance

A. The Data Governance Policy applies to all users of Attalla 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 Attalla 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 Attalla City Schools' policies. Further, penalties associated with state and federal laws may apply.

B. 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 Attalla City School technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Attalla 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.

Appendices

Laws, Statutory, Regulatory, and Contractual Security Requirements

Appendix A

A. **CIPA:** The Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

   For more information, see: http://www.fcc.gov/guides/childrens-internet-protection-act

B. **COPPA:** The Children's Online Privacy Protection Act, regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information.

   For more information, see: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

C. **FERPA:** The Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

   For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

D. **HIPAA:** The Health Insurance Portability and Accountability Act, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

   For more information, see: http://www.hhs.gov/ocr/privacy/hipaa/understanding/

   In general, schools are not bound by HIPAA guidelines.

E. **PCI DSS:** The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.

   For more information, see: www.pcisecuritystandards.org

F. **PPRA:** The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

These include the right to the following:

Consent before students are required to submit to a survey that concerns one or more of the following protected areas ("protected information survey") if the survey is funded in whole or in part by a program of the U.S. Department of Education (ED)-

1. Political affiliations or beliefs of the student or student's parent;
2. Mental or psychological problems of the student or student's family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating, or demeaning behavior;
5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
7. Religious practices, affiliations, or beliefs of the student or parents; or
8. Income, other than as required by law to determine program eligibility.

Receive notice and an opportunity to opt a student out of-

1. Any other protected information survey, regardless of funding;
2. Any non-emergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under State law; and
3. Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Information Risk Management Practices

Appendix B

The analysis involved in Attalla City Schools Risk Management Practices examines the types of threats - internal or external, natural or manmade, electronic and non-electronic - that affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which potentially exposes the information resource to the threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined and addressed based on recommendations by the Data Governance Committee. The frequency of the risk analysis is determined at the district level. It is the option of the superintendent or designee to conduct the analysis internally or externally.

Definitions and Responsibilities

Appendix C

Definitions

A. **Availability:** Data or information is accessible and usable upon demand by an authorized person.
B. **Confidentiality:** Data or information is not made available or disclosed to unauthorized persons or processes.
C. **Data:** Facts or information
D. **Entity:** Organization such as school system, school, department, or in some cases a business
E. **Information:** Knowledge that you get about something or someone; facts or details.
F. **Data Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.
G. **Involved Persons:** Every user of Involved Systems (see below) at Attalla City Schools - no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
H. **Systems:** All data-involved computer equipment/devices and network systems that are operated within or by the Attalla City Schools physically or virtually. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
I. **Personally Identifiable Information (PII):** PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
J. **Risk:** The probability of a loss of confidentiality, integrity, or availability of information resources.

Responsibilities

A. **Data Governance Committee:** The Data Governance Committee for Attalla City Schools is responsible for working with the Information Security Officer (ISO) to ensure security policies, procedures, and standards are in place and adhered to by the entity. Other responsibilities include:

    1. Reviewing the Data Governance Policy annually and communicating changes in policy to all involved parties.
    2. Educating data custodians and managing owners and users with comprehensive information about security controls affecting system users and application systems.

B. **Information Security Officer:** The Information Security Officer (ISO) for Attalla City Schools is responsible for working with the superintendent, Data Governance Committee, user management, owners, data custodians, and users to develop and implement prudent security policies, procedures, and controls. Specific responsibilities include:

1. Providing basic security support for all systems and users.
2. Advising owners in the identification and classification of technology and data related resources.
   See also Appendix D (Data Classification Levels)
3. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
4. Performing or overseeing security audits.
5. Reporting regularly to the superintendent and Attalla City Schools Data Governance Committee on Attalla City Schools' status with regard to information security.

C. **User Management:** Attalla City Schools' administrators are responsible for overseeing their staff use of information and systems, including:

1. Reviewing and approving all requests for their employees' access authorizations.
2. Initiating security change requests to keep employees' secure access current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the ISO and the Data Governance Committee the loss or misuse of Attalla City Schools' information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any technology or data system/software to manage information.
9. Following all privacy and security policies and procedures.

D. **Information Owner:** The owner of a collection of information is usually the administrator or supervisor responsible for the creation of that information. In some cases, the owner may be the primary user of that information. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the Attalla City Schools Information Owner Delegation/Transfer Request Form and submitting the form to the Data Governance Committee for approval. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on ALSDE guidelines, industry standards, Data Governance Committee guidelines, or advice from the school system attorney.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.

4. Authorizing access and assigning data custodianship if applicable.
5. Specifying controls and communicating the control requirements to the data custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of Attalla City Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organizational unit and district for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

E. **Data Custodian:** The data custodian is assigned by an administrator, data owner, or the ISO based on his/her role and is generally responsible for the processing and storage of the information. The data custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the ISO and/or Data Governance Committee for use and disclosure using procedures that protect the privacy of the information.
5. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO and/or Data Governance Committee.
6. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
7. Reporting promptly to the ISO and/or Data Governance Committee the loss or misuse of Attalla City Schools data.
8. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

F. **User:** The user is any person who has been authorized to read, enter, print or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.
2. Comply with all data security procedures and guidelines in the Attalla City Schools Data Governance Policy and all controls established by the data owner and/or data custodian.
3. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
4. Report promptly to the ISO and/or Data Governance Committee the loss or misuse of Attalla City Schools' information.
5. Follow corrective actions when problems are identified.

Data Classification Levels

Appendix D

A. **Personally Identifiable Information (PII)**

1. PII is information about an individual maintained by an agency, including:
    a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
    b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications for Attalla City Schools.

B. **Confidential Information**

1. Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access.

    Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Attalla City Schools, its staff, parents, students including contract employees, or its business partners. Decisions about the provision of access to this information shall always be cleared through the information owner and/or Data Governance Committee.

C. **Internal Information**

1. Internal Information is intended for unrestricted use within Attalla City Schools, and in some cases within affiliated organizations such as Attalla City Schools' business or community partners. This type of information is already widely-distributed within Attalla City Schools, or it could be so distributed within the organization without advance permission from the information owner.

    Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PII, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. **Public Information**

1. Public Information has been specifically approved for public release by a designated authority within each entity of Attalla City Schools. Examples of Public Information may include marketing brochures and material posted to Attalla City Schools' web pages.
2. This information may be disclosed outside of Attalla City Schools.

E. **Directory Information**

Attalla City Schools defines Directory information as follows:

1. Student first and last name
2. Student gender
3. Student home address
4. Student homeroom
5. Student home telephone number
6. Student school-assigned monitored and filtered email address
7. Student photograph
8. Student place and date of birth
9. Student dates of attendance (years)
10. Student grade level
11. Student diplomas, honors, awards received
12. Student participation in school activities or school sports
13. Student weight and height for members of school athletic teams
14. Student most recent institution/school attended
15. Student ID number

Acquisition of Software Procedures

Appendix E

The purpose of the Acquisition of Software Procedures is to:

- Ensure proper management of the legality of information systems,
- Allow all academic disciplines, administrative functions, and athletic activities the ability to utilize proper software tools,
- Minimize licensing costs,
- Increase data integration capability and efficiency of Attalla City Schools (ACS) as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

A. **Software Licensing:**

1. All district software licenses owned by ACS will be:
    - kept on file at the central office,
    - accurate, up to date, and adequate, and
    - in compliance with all copyright laws and regulations
2. All other software licenses owned by departments or local schools will be:
    - kept on file with the department or local school technology office,
    - accurate, up to date, and adequate, and
    - in compliance with all copyright laws and regulations
3. Software installed on ACS technological systems and other electronic devices:
    - will have proper licensing on record,
    - will be properly licensed or removed from the system or device, and
    - will be the responsibility of each ACS employee purchasing and installing to ensure proper licensing
4. Purchased software accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) on file that states or confirms at a minimum that:
    - ACS student and/or staff data will not be shared, sold, or mined with or by a third party,
    - ACS student and/or staff data will not be stored on servers outside the US unless otherwise approved by Attalla City Schools' Data Governance Committee,
    - the company will comply with ACS guidelines for data transfer or destruction when contractual agreement is terminated, and
    - No API will be implemented without full consent of ACS and the ALSDE.
5. Software with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly evaluated and licensed if necessary and is applicable to this procedure. It is the responsibility of staff to ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use. Staff members are responsible for ensuring that parents have given permission for staff to act as their agent when creating student accounts for online resources.

B. **Supported Software:**

In an attempt to prevent software containing malware, viruses, or other security risks, software is categorized as Supported and Not Supported Software. For software to be classified as Supported Software downloads and/or purchases shall be approved by the district technology Director or designee.

1. A list of supported software will be maintained on the ACS District Technology site.
2. It is the responsibility of the ACS Technology Team members to keep the list current and for staff to submit apps or other software to the Technology Team.
3. Unsupported software is considered New Software and shall be approved or it will not be allowed on ACS owned devices.
4. When staff recommends apps for the ACS Mobile Device Management Apps Catalog or software for installation, it is assumed that the staff has properly vetted the app or software and that it is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.
5. Software that accompanies adopted instructional materials will be vetted by the Curriculum and Instruction Director and the Technology Director and is therefore supported.

C. **New Software:**

In the Evaluate and Test Software Packages phase, the software will be evaluated against current standards and viability of implementation into the ACS technology environment and the functionality of the software for the specific discipline or service it will perform.

1. Evaluation may include but is not limited to the following:
    - Conducting beta testing.
    - Determining how the software will impact the ACS technology environment such as storage, bandwidth, etc.
    - Determining hardware requirements.
    - Determining what additional hardware is required to support a particular software package.
    - Outlining the license requirements/structure, number of licenses needed, and renewals.
2. Determining any Maintenance Agreements including cost.
    - Determining how the software is updated and maintained by the vendor.
    - Determining funding for the initial purchase and continued licenses and maintenance.
3. When staff recommends apps for the ACS Mobile Device Management Apps Catalog or software for purchase and/or testing, it is the responsibility of the appropriate staff to properly vet the app or software to ensure that it is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.

Virus, Malware, Spyware, Phishing, and SPAM Protection

Appendix F

Virus, Malware, and Spyware Protection

Attalla City desktops, laptops, and file servers run Sophos Endpoint Protection. Virus definitions are updated in real time as they become available and an on access scan is performed on all "read" files continuously. Reports from scans are monitored daily, and statuses are corrected, when needed.

Internet Filtering

Student learning using online content and social collaboration continues to increase. Attalla City Schools views Internet filtering as a way to balance safety with learning-letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and app use with student safety and network security, the Internet traffic from all devices that authenticate to the network is routed through the iBoss filter using the user's network credentials. For district-owned devices, this happens transparently at the Windows login screen. For personal devices, users connect to the “ACS-Employees” wireless network that is secured with 802.1x authentication that requires them to login to the wireless network using their network credentials. This authentication is passed on to the iBoss Internet filter for proper Internet filtering policy assignment based on the user. Guests of Attalla City Schools connect their personal devices to the “ACS-GuestSecure” wireless network and accept a user agreement at a “click-through splash page”. The Guest network is filtered at a very tight level and is the same for all guests that choose to connect. This process sets the filtering level appropriately based on the role of the user, such as, student, staff or guest. More specifically for students, the grade level of the child is also taken into consideration when assigning age appropriate Internet filtering policies. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

In addition to the built-in spam filtering for Gmail, email is also filtered for viruses, phishing, spam, and spoofing using Gmail’s email security features.

Security Patches

Windows security patches and other Windows patches are scheduled to "auto-download" and "schedule install." The scheduled install occurs during the following maintenance window: Monday-Friday 4:00 a.m. to 5:30 a.m. File Servers are scheduled to "auto-download" and are updated automatically on Saturdays at 2:00 a.m. after which the file server is automatically rebooted.

Physical and Security Controls

Appendix G

The following physical and security controls shall be adhered to:

1. Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
2. Monitor and maintain data centers' temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
3. File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
4. Computers and other systems shall 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.
5. 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.
6. Maintain a log of all visitors granted entry into secured areas or 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.
7. Monitor and control the delivery and removal of all asset-tagged and/or data-storing technological equipment or systems. 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 shall be moved without the explicit approval of the technology department.
8. Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

See also Appendix I (Purchasing and Disposal Procedures)

Password Control Standards

Appendix H

The Attalla City Schools Data Governance and Use Policy requires the use of strictly controlled passwords for network access and for access to secure sites and information. In addition, all users are assigned to Microsoft security groups that are managed through Microsoft Group Policies. The security groups include separate groups at each school for Office Staff, Tech Staff, Instructional Staff, Students, and Users.

Password Standards:

A. **Users are responsible for complying with the following password standards for network access or access to secure information:**

1. Passwords shall never be shared with another person, unless the person is a designated security manager.
2. Every password shall, where possible, be changed yearly if not more frequently for staff and on an age appropriate schedule for students.
3. Passwords shall, where possible, have a minimum length of eight (8) characters.
4. When possible, for secure sites and/or software applications, user created passwords should adhere to the same criteria as required for network access. This criteria is defined in the ACS Network Group Policy Criteria for Passwords and is listed below:
    a. Shall not contain the user's account name or parts of the user's full name that exceed two consecutive characters
    b. Contain characters from three of the following four categories:
        i. English uppercase characters (A through Z)
        ii. English lowercase characters (a through z)
        iii. Base 10 digits (0 through 9)
        iv. Non-alphabetic characters (for example, !, $, #, %)
5. Passwords shall never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the Technology Department. This feature shall be disabled in all applicable systems.
6. Passwords shall not be programmed into a PC or recorded anywhere that someone may find and use them.
7. When creating a password for secure information or sites, it is important not to use passwords that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc.). A combination of alpha and numeric characters is more difficult to guess.

B. **Where possible, system software should enforce the following password standards:**

1. Passwords routed over a network shall be encrypted.
2. Passwords shall be entered in a non-display field.
3. System software shall enforce the changing of passwords and the minimum length.
4. System software shall disable the user password when more than five consecutive invalid passwords are given. Lockout time shall be set at a minimum of 30 minutes.

5. System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user. A combination of alpha and numeric characters is more difficult to guess.

Purchasing and Disposal Procedures

Appendix I

This procedure is intended to provide for the proper purchasing and disposal of technological devices only. 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 in this document. For further clarification of the term technological systems contact the Attalla City Schools' (ACS) district Technology Director.

All involved systems and information are assets of Attalla City Schools and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Purchasing Guidelines**

All systems that will be used in conjunction with Attalla City Schools' technology resources or purchased, regardless of funding, shall be purchased from an approved list or be approved by the district Technology Director. Failure to have the purchase approved may result in lack of technical support, request for removal from premises, or denied access to other technology resources.

B. **Alabama Competitive Bid Laws**

All electronic equipment is subject to Alabama competitive bid laws. There are several purchasing coops that have been approved for use by the Alabama State Examiners office: http://www.examiners.state.al.us/purchcoop.aspx. Generally for technological devices and services, Attalla City Schools purchase from the Alabama Joint Purchasing Agreement (ALJP): https://connect.alsde.edu/sites/eia/aljp/SitePages/ALJP%20(Alabama%20K-12%20(IT)%20Joint%20Purchasing)Home.aspx. In the event that a desired product is not included in one of these agreements, Attalla City Schools bids the item or items using the district's competitive bid process. All technological systems, services, etc. over $15,000 purchased with public funds are subject to Alabama's competitive bid laws.

C. **Inventory**

All technological devices or systems over $500 are inventoried by the Technology Department in accordance with the Attalla City Schools' Finance Department using the WASP inventory system. There are some exceptions under $500, as determined by the Technology Director, such as but not limited to companion devices or peripherals that are inventoried. It is the responsibility of the local school technology contact to inventory technological systems used in the local school and manage said inventory. The district technology staff is responsible for ensuring that any network equipment, file servers, or district systems, etc. are inventoried.

D. **Disposal Guidelines**

Equipment shall be considered for disposal for the following reasons:

1. End of useful life,
2. Lack of continued need,
3. Obsolescence,
4. Wear, damage, or deterioration,
5. Excessive cost of maintenance or repair.

The local school principal, Technology Director, and the Chief Financial Officer shall approve school disposals by discard or donation. Written documentation in the form of a spreadsheet including but not limited to the following shall be provided to the District Technology Office no later than Monday at 9:00 a.m. prior to the next Board of Education meeting on the following Thursday:

1. Fixed asset tag (FAT) number,
2. Location,
3. Description,
4. Serial number, and
5. Original cost and account code if available.

E. **Methods of Disposal**

Once equipment has been designated and approved for disposal, it shall be handled according to one of the following methods. It is the responsibility of the local school technology contact to modify the WASP inventory entry to reflect any in-school transfers, in-district transfers, donations, or discards for technological systems. The district technology staff is responsible for modifying the inventory records to reflect any transfers within the central offices, transfers of central office electronic equipment to local schools, central office donations, or central office discards.

1. **Transfer/Redistribution**
   If the equipment has not reached the end of its estimated life, an effort shall be made to redistribute the equipment to locations where it can be of use, first within an individual school or office, and then within the district. Service requests may be entered to have the equipment moved, reinstalled and, in the case of computers, laptops, or companion devices, have it wiped and reimaged or re-configured.

2. **Discard**
   All electronic equipment in the Attalla City Schools district shall be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district. A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation

verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data. Under no circumstances should any technological systems/equipment be placed in the trash. Doing so may make Attalla City Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

3. **Donation**
   If the equipment is in good working order, but no longer meets the requirements of the site where it is located and cannot be put into use in another part of a school or system, it may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's director.

   It shall be made clear to any school or organization receiving donated equipment that ACS is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

   ACS staff should make every effort before offering donated equipment, to make sure that it is in good condition and can be reused. Microsoft licenses or any other software licenses are not transferred outside the Attalla City School system.

   Donations are prohibited to individuals outside of the school system or to current faculty, staff, or students of Attalla City Schools. The donation of or sale of portable technology-related equipment is permissible to retiring employees if the following criteria have been met:

   a. the portable equipment has been used solely by the retiring employee for over two years;
   b. the equipment will not be used by the employee assuming the responsibilities of the retiring employee; and
   c. the equipment has reached or exceeded its estimated life.

   All donations and/or sales shall be approved by the Chief Financial Officer and Technology Director.

F. **Required Documentation and Procedures**

1. For purchases, transfers and redistributions, donations, and disposal of technology-related equipment, it is the responsibility of the appropriate technology team member to create/update the inventory to include previous location, new school and/or room location, and to note the transfer or disposal information. When discarding equipment, the fixed asset tag is removed from the equipment and turned in with other documentation to the local school bookkeeper. A spreadsheet export from WASP is sent to the district technology office. The Technology Director in turns submits to the CFO for approval and to the Superintendent's Office for Board approval.
2. When equipment is donated, a copy of the letter requesting the equipment shall be on-file with the district technology office prior to the donation. Equipment is donated in order of request.

3. Any equipment donated shall be completely wiped of all data. This step will not only ensure that no confidential information is released, but also will ensure that no software licensing violations will inadvertently occur. For non-sensitive machines, all hard drives shall be fully wiped using a wiping program approved by the district technology office, followed by a manual scan of the drive to verify that zeros were written.
4. Any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts shall be removed: special adapter cards, memory, hard drives, zip drives, CD drives, etc.
5. A district-approved vendor shall handle all disposals that are not redistributions, transfers, or donations. Equipment shall be stored in a central location prior to pick-up. Summary forms shall be turned into district technology office and approved by the Chief Financial Officer prior to the scheduled "pick up" day. Mice, keyboards, and other small peripherals may be boxed together and shall not be listed on summary forms.

Data Access Roles and Permissions

Appendix J

Attalla City Schools maintain the following security permission groups in PowerSchool:

Group Name	Access Level	Members
Teacher (1)	View	Teachers
SIS Admin with DDA (9)	View and Modify	Technology Director; Data Manager
SIS Admin no DDA (10)	View and Modify	As needed
Administrator (11)	View and Modify	District Directors; Responsible for the upkeep, configuration, and reliable operation at the district level
School Level Administrator (12)	View and Modify	Principals and Assistant Principals, Afterschool, Tutoring, Special Education (Access to all students' records) Responsible for the upkeep, configuration, and reliable operation at the school level
Counselor (13)	View	School Counselors
Secretary (15)	View and Modify	School secretaries, bookkeepers, office staff
Nurse (21)	View and Modify	Nurses
Nurse Sub (22)	View	Substitute Nurses (can add to health records)
Instructional Partner (23)	View and Modify	Instructional Partners
ACCESS (24)	View	ACCESS Facilitators and Career Coaches
Superintendent (25)	View and Modify	Superintendent
Special Education (View Only) (26)	View	Special Programs Role *Do Not Touch
Special Education Administrator (27)	View and Modify	Special Programs Role *Do Not Touch
Read-Only Export (Clever) (28)	View	Clever *Do Not Touch
CNP (29)	View	Lunchroom Managers
Special Programs-District (30)	View	District Special Education Staff
Social Worker (32)	View	Social Worker
SRO (34)	View	SROs

Attalla City Schools Technological Services and Systems

Memorandum of Agreement (MOA)

Appendix K

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the ___ day of _____, 20__, by and between _____, a corporation organized and existing under the laws of _____ (the "Company"), and **ATTALLA CITY SCHOOLS (ACS)**, a public school system organized and existing under the laws of the state of Alabama (the "School Board"), recites and provides as follows.

Recitals

The Company and the School Board are parties to a certain agreement entitled "_____" hereafter referred to as (the "Agreement"). In connection with the execution and delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student Personally Identifiable Information (PII) hereafter referred to as student information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

Agreement

The following provisions shall be deemed to be included in the Agreement:

Confidentiality Obligations Applicable to Certain ACS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all ACS student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information will not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

The Company shall cause each officer, director, employee and other representative who shall have access to ACS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all ACS Student Information. The Company shall take all reasonable steps to insure that no ACS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for ACS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of ACS, or (c) are entitled to such ACS student information from the Company pursuant to federal and/or Alabama law. The Company shall use ACS student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information,

solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the ACS student information as confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Alabama law; (c) maintain at all times a list of Authorized Representatives with access to ACS student information.

Other Security Requirements. The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of ACS student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to email, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify ACS of planned system changes that may impact the security of ACS data; (g) return or destroy ACS data that exceed specified retention schedules; (h) notify ACS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of ACS information to the previous business day. The Company should guarantee that ACS data will not be sold to, accessed by, or moved by third parties.

In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify ACS within 24 hours of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the ACS student information compromised by the breach; (c) return compromised ACS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with ACS efforts to communicate to affected parties by providing ACS with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with ACS to remediate the breach which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the disclosure; (f) cooperate with ACS by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide ACS with notice within 24 hours of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of ACS data of any kind, failure to follow security requirements and/or failure to safeguard ACS data. The Company's compliance with the standards of this provision is subject to verification by ACS personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and shall not be shared, sold, or moved to other companies or organizations nor should other companies or organizations be allowed access to said information.

Disposition of ACS Data Upon Termination of Agreement

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required ACS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to ACS data and of fulfilling its obligations pursuant to

this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be school officials of the School Board, and shall maintain ACS data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in ACS data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of its officers, directors, employees, agents or representatives of the obligations of the Company or its Authorized Representatives under this provision.

Certain Representations and Warranties. The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company's execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

Governing Law; Venue. Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Alabama, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Alabama.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

[COMPANY NAME]

By:_____
[Name]
[Title]

ATTALLA CITY SCHOOLS

By: Jeff Colegrove
Jeff Colegrove
Superintendent
Attalla City Schools

Attalla City Schools IT Disaster Recovery Plan

Appendix L

A. Purpose

The purpose of this policy is to clearly define roles and responsibilities for the reporting, investigation and response of computer security incidents and data breaches.

B. Scope

This policy applies to information systems, regardless of ownership or location, used to store, process, transmit or access Attalla City Schools (ACS) data as well as all personnel including employees, students, temporary workers, contractors, those employed by contracted entities and others authorized to access ACS enterprise assets and information resources.

ACS data includes, but is not limited to, the following: personnel data, student data (FERPA), protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA) regulation, and controlled unclassified information (CUI).

C. Policy

The Attalla City Schools' Cyber Risk Team (CRT) consists of the technology director, technology staff, superintendent, SROs, and other district personnel. The CRT investigates security events to determine whether an incident has occurred and the extent, cause and damage of incidents.

The CRT directs the recovery, containment, and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The CRT coordinates response with external parties when existing agreements place responsibility for incident investigations on the external party.

During the conduct of security incident investigations, the CRT is authorized to monitor relevant ACS IT resources and retrieve communications and other relevant records of specific users of ACS IT resources, including login session data and the content of individual communications without notice or further approval.

Any external disclosure of information regarding information security incidents must be reviewed and approved by the Board of Education and/or system attorney.

The CRT coordinates with law enforcement, government agencies, peer CRTs and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. The CRT may share threat and incident information with these organizations that do not identify any member of the ACS community.

D. Responsibilities

All members of the ACS community are responsible for promptly reporting any suspected or confirmed security incident involving ACS data or an associated information system, even if they have contributed in some way to the event or incident.

Members of the ACS community must cooperate and assist with incident investigations and encourage their staff and others to report an incident and cooperate with an investigation.

E. Information Security Incidents

All suspected information security (IS) incidents must be reported. The following courses of action need to be taken in the event of discovering an information security incident:

If the incident involves Protected Health Information (PHI) in electronic or paper form:

1. Call the Attalla City Schools Director of Technology at (256) 538-8051.
2. If unavailable, notify a member of the Technology Department, Superintendent, or School Administrator
3. It is highly recommended to make an immediate phone call and not email. Include particular information if the incident involves:
    a. Inadvertent release, exposure, or compromise of confidential data, the loss or compromise of portable computing devices or removable media containing sensitive data, or the discovery of unauthorized access to sensitive data on a computer or data storage device.
    b. The use of ACS computing resources in the commission of fraudulent activities.
    c. Systems used to process or store Controlled Unclassified Information (CUI).

If the suspected incident involves any of the following, the Information Security Department will work to also report:

1. Credit or debit card account information
2. Protected Health Information (PHI), in electronic or paper form
3. Fraudulent activity committed using ACS computing resources
4. Criminal activity committed using ACS computing resources
5. Controlled Unclassified Information (CUI) related incident (systems and/or data)
6. FERPA does not require data breach disclosure but the ACS Director of Technology should be contacted.

When a subpoena or court order is issued pursuant to any investigation related to information technology the superintendent will notify the board attorney and will direct the actions to be taken.

Police and the Attorney's Office will serve as liaison with all external law enforcement agencies (FBI, other federal, state, local) for all IT security investigations.

ACS encourages stakeholders to report other concerns, suspected violations, or criminal activity to their supervisor or other campus entities as appropriate.

School administrators are responsible for dissemination of this policy to their departments. The Cyber Response Team (CRT) is responsible for responding to High Severity incidents according to established procedures.

The Director of Technology is responsible for coordinating the CRT and augments staff with subject matter experts as necessary.

Creation Date: March 15, 2022
Board Approved: April 14, 2022

Resources

ALSDE State Monitoring Checklist

Resource 1

Data Governance					
A. Data Governance and Use Policy					
ON-SITE	**YES**	**NO**	**N/A**	**Indicators**	**Notes**
1. Has a data governance committee been established and roles and responsibilities at various levels specified?				• Dated minutes of meetings and agendas • Current list of roles and responsibilities	
2. Has the local school board adopted a data governance and use policy?				• Copy of the adopted data governance and use policy • Dated minutes of meetings and agenda	
3. Does the data governance policy address physical security?				• Documented physical security measures	
4. Does the data governance policy address access controls and possible sanctions?				• Current list of controls • Employee policy with possible sanctions	
5. Does the data governance policy address data quality?				• Procedures to ensure that data are accurate, complete, timely, and relevant	
6. Does the data governance policy address data exchange and reporting?				• Policies and procedures to guide decisions about data exchange and reporting • Contracts or MOAs involving data exchange	
7. Has the data governance policy been documented and communicated in an open and accessible way to all stakeholders?				• Documented methods of distribution to include who was contacted and how • Professional development for all who have access to PII	

Record Disposition Requirements

Resource 2

The information below is from the Local Boards of Education Records Disposition Authority approved by the Local Government Records Commission, October 2, 2009. The complete document can be found at: http://www.archives.alabama.gov/officials/localrda.html.

The following sections are of special interests:

1.04 Administrative Correspondence

4.02 20-Day Average Daily Membership Reports

4.04 Principals Attendance Reports

6.01 Student Handbooks

6.03 Daily/Weekly Teacher Lesson Plans

9.14 Websites

10.04 Purchasing Records

10.05 Records of Formal Bids

10.06 Contracts

10.08 Grant Project Files

Email Guidelines

Resource 3

The purpose of these guidelines is to ensure the proper use of Attalla City Schools' email and Internet communication systems and to make users aware of what Attalla City Schools deems acceptable and unacceptable use of its email and Internet communication systems. We reserve the right to amend these guidelines as necessary. In case of revisions, users will be informed by email, by posting on the District Technology web page, through professional development, at faculty meetings, grade level meetings, or department meetings, assemblies, in class, and/or by other means deemed appropriate by the administration.

Email

Legal Risks

Email is a school business or educational communication tool, and users are obliged to use this tool in a responsible, effective, and lawful manner. Email lends itself to a kind of informality yet, from a legal perspective, may have the same implications as would any written communication. Any email is discoverable in a due process situation or other legal action. In addition, any email exchanged by a school system employee is public record. Other legal risks of email for Attalla City Schools and/or their network users include the following:

1. sending emails with any libelous, defamatory, offensive, racist or obscene remarks;
2. forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks;
3. transmitting or forwarding confidential information;
4. forwarding or copying messages without permission or implied permission; and/or
5. knowingly sending an attachment that contains a virus that severely affects another network or other users

By following the guidelines in this document, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in these guidelines, the user will be fully liable and Attalla City Schools will disassociate itself from the user as far as legally possible.

1. Do not send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email containing libelous, defamatory, offensive, racist or obscene remarks, promptly notify your supervisor.
2. Use caution if you forward a message without implied permission or without acquiring permission from the sender first, especially if it contains sensitive or private information.
3. Do not forge or attempt to forge email messages.
4. Do not send email messages using another person's or a bogus email account.
5. Do not copy a message or attachment belonging to another user without the permission or implied permission of the originator.
6. Do not disguise or attempt to disguise your identity when sending email.

Best Practices

Attalla City Schools considers email as an important means of communication and recognizes the importance of proper email content and of speedy replies in conveying a professional image and in delivering good service. The use of email in education, however, is proliferating and the precise legal issues regarding appropriate use are yet to be determined. We are confident that-

1. Any email exchanged by school system employees about individual students is public record.
2. Any email pertaining to a particular student is discoverable in a due process situation or other legal action.
3. The nature of email lends itself to impulsive, overly informal, and sometimes unprofessional communication.

Therefore Attalla City Schools urges users to adhere to the following guidelines:

Guidance on Email between School Employees and Parents/Guardians

Examples of generally appropriate use of email between school employees and parents/guardians:

1. Teachers invite parents to provide email addresses and then send out emails to those addresses reporting on classroom activities, projects, and assignments. These messages are generic and do not refer to specific students.
2. Teachers may initiate or respond to email from a parent or guardian about a specific child, exchanging objective not subjective information such as the student's attendance, participation, homework, and performance in class.

Examples of inappropriate use of email between school employees and parents/guardians:

1. Using email to report on serious problems regarding individual students.
2. Using email to discuss confidential and sensitive matters, including:
    a. Medical/psychiatric/psychological diagnoses and treatments.
    b. Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters.
    c. Family problems and other sensitive family information.
3. Using language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
    a. "Have you considered that Johnny might have ADHD?"
    b. "Overall, I think that Johnny is unmotivated/lazy."
    c. "I don't think there is anything wrong with Johnny except his negative attitude."

Email between teachers and parents shall be positive and/or general in nature when possible. Discussions involving serious problems and any and all protected information (medical, psychological, psychiatric, Special Education, and Section 504, and disciplinary matters) should occur in person or by telephone.

Parents may initiate inappropriate email exchanges. Example: "Johnny is in your American History class and is failing. His father is an alcoholic and we are divorced. Johnny has ADHD and clinical depression. Can you please tell me how he is doing in your class and what I can do to help him?"

That kind of message shall be deleted and the teacher receiving it should call the parent who sent it. Alternately, the teacher could reply to it, deleting everything from the body of the email sent by the parent, and then respond with directions about how the teacher can be reached by telephone or in person. Do not regard a parent or guardian's initiation of this kind of email exchange as constituting permission for you to discuss these matters via email.

Guidance on Email between School Employees Concerning Students

Examples of generally appropriate use of email between school employees:

1. Emails which provide positive information, objective comments, and/or neutral information regarding school performance. In other words, conducting straight-forward business, staying away from sensitive and confidential areas.

Examples of inappropriate use of email between school employees:

1. Using email to report on serious problems regarding individual students.
2. Using email to discuss confidential and sensitive matters, including
    a. Medical/psychiatric/psychological diagnoses and treatments.
    b. Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters.
    c. Family problems and other sensitive family information.
3. Using, in email, language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
    a. "I think Johnny has ADHD"
    b. "Overall, I think that Johnny is unmotivated/lazy"
    c. "I don't think there is anything wrong with Johnny except his negative attitude."
    d. "I think this child's problem is his home life."

Discussions involving severe problems, subjective comments, and any and all protected information (medical, psychological, psychiatric, Special Education, and Section 504, and disciplinary matters) should occur in person or by telephone.

General Best Practices involving all email are as follows:

<u>Writing emails:</u>

1. Use short, descriptive Subject: lines.
2. Avoid lengthy, detailed email messages. Consider using an attachment for "How To" information, directions, procedures, processes, or similar types of information.
3. Avoid unnecessary attachments or large file attachments such as multiple pictures, mini movies, etc. AVOID USING ALL CAPITALS.
4. If using cc or bcc features, take steps to inform the cc or bcc recipient of any action expected unless the action is explicit in the email. The bcc option is often used to avoid revealing recipient email addresses to the entire group receiving the email; otherwise, the bcc option shall be used sparingly if at all.
5. If you forward emails, state clearly what action you expect the recipient to take.
6. Use the spell checker before you send out an email.
7. If the content of an email is not of a public nature, consider using another form of communication or protect the information by using a password.
8. Only mark emails as important if they really are important.

Replying to emails:

1. Emails shall be answered within 24 hours, and at minimum employees are expected to check email at least once per day.
2. Responses shall not reveal confidential information and shall be professional.

Electronic Social Networking, Instant Messaging including Texting, etc.

Electronic social networking and/or instant messaging, such as but not limited to Facebook, Instagram, Twitter, IM, or texting, among staff and students is a particularly sensitive matter in a time when growing numbers of school employees maintain social networking accounts, email extensively in their personal lives, and are accustomed to using instant messaging services.

An absolute prohibition of communicating electronically with students seems excessive. On the other hand, teachers and school staff shall maintain the highest standards should they choose to interact with students through electronic media. Below are some typical situations in which employees might need guidance.

Guidelines below are presented in a Q&A format.

Q: Is it ok for me to initiate electronic communications with a student?

A: If a teacher initiates overly personal contact with students outside of school, whether in person or electronically, he or she may create an impression of an unhealthy interest in that student's personal life and may leave himself or herself open to an accusation of inappropriate conduct. Therefore, caution shall be exercised in this type of communication.

Q: What if I receive an email or other electronic message such as a text from a student?

A: This very much depends on the nature of the communication received. We would strongly discourage any use of texting, instant messaging or "chat"-type communication with students for purposes other than school related communications. Do not engage in social "chat" with students. If a communication is received which appears to be a social greeting, you might do best just to acknowledge it in an appropriate way at school. A very brief acknowledging electronic response might be appropriate in some circumstances. However, it is perfectly OK not to respond to such greetings. If you choose not to respond, making an extra effort to cheerfully greet the student at school might be appropriate.

If a student sends a message with disturbing content, you should discuss this with your administrator or supervisor, including a school counselor in the discussion as needed.

If a student sends a message that appears to suggest an emergency (an allegation of abuse or a student sharing suicidal thoughts or plans), try to contact your administrator or supervisor at once.

Q: What about Facebook accounts or other social networking sites? Should I respond to an invitation to become a student's "Friend" or follow their account/the student follow my account??

A: We recommend that you not engage in online social networking with students unless the site is used for school information or academic reasons only. This would only be an issue, of course, if you choose to maintain a Facebook, or similar social networking account. If you do so, we recommend that you be extremely cautious about the content of your profiles and pages.

If you are strictly using a social networking site for school related topics and stay away from personal content then these sites shall be treated much like any other educational blog. (However, the use of comments, "writing on walls," and so on, would be likely to lead to major problems if an approval process is not in place before posting.) You may find that it is easier to simply tell your students that you have a policy not to accept students as "friends" or "followers".

General Email Information

Virus Protection and Filtering
Incoming and outgoing emails sent to or received from Attalla City Schools' Exchange email server are scanned for viruses, spam, and content. However, users are expected to exercise caution when opening emails from unknown users or when using the web-based email client from home computers.

1. Incoming emails may be blocked if the message size and/or attachments are too large, inappropriate, or potentially harmful.

Disclaimer
Attalla City Schools recommends that employees add a disclaimer to outgoing emails or automatically attach a disclaimer such as the one below to each email sent outside the school system.

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Attalla City Schools. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email."

System Monitoring
Although Attalla City Board policy permits personal use of school email accounts, users shall have no expectation of privacy in anything they create, store, send or receive on the Attalla City Schools' computer system. Emails may be monitored without prior notification if Attalla City Schools deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, Attalla City Schools reserves the right to take disciplinary action, including termination and/or legal action.

Email Accounts
Email accounts are assigned to new employees when their employment is approved by the Board of Education and when the new employee has read and signed acknowledgement and understanding of the Attalla City Schools Technology Usage Policy. All email accounts maintained on the Attalla City email and Internet communication systems are property of Attalla City Schools. Attalla City maintains student accounts, employee accounts, and employee-sponsored accounts.

Passwords shall not be given to other people and shall be changed if the user believes his/her password is no longer secure. Email accounts are deleted immediately when employees retire, resign, or take leave from the school system for a period of six months or more. Only Attalla City employees are given email accounts. Upon request by the administration, Attalla City employee sponsored accounts, such as PTA accounts or accounts for contract employees may be created. Employee-sponsored accounts are subject

to these guidelines and it is the responsibility of the sponsoring employee to educate the user of this and all other relevant technology-related policies and guidelines.

Electronic Communications for Personal Use
Although Attalla City Schools' email and Internet communication systems is meant for school business, Attalla City Schools allows the reasonable use of email for personal use if certain guidelines are adhered to:

1. Personal use of email shall not interfere with work.
2. Personal emails shall also adhere to the guidelines in this policy.
3. Personal emails shall be deleted regularly so as not to clog the system.

The forwarding of chain letters, junk mail, inappropriate jokes, and executable files is strictly forbidden.

1. Do not send personal mass mailings.
2. Do not send emails for personal gain, to solicit business for friends, family, etc., or for political purposes.
3. All messages distributed via the school system's email and Internet communication systems, even personal emails, are Attalla City Schools' property.
4. Recognize the diversity of co-workers when sending emails. For example, some employees would regard emails of a religious nature, including invitations to religious events or services - even prayer requests - as inappropriate or offensive.

Questions
If you have any questions or comments about these guidelines, please contact your principal, immediate supervisor, or the district technology director. If you do not have any questions Attalla City Schools presume that you understand and are aware of the rules and guidelines and will adhere to them.

Agreements for Contract Employees Including Long-Term Substitutes

Resource 4

Procedure:

1. All contract employees, including those from any third-party staffing/personnel services, should complete the following prior to gaining access to the Attalla City Schools Network, PowerSchool, PS Special Programs, and email (if applicable):

    A. Read and sign to acknowledge the **Technology Usage Policy, and complete the Data Governance online training.**

        a. Form available on attalla.k12.al.us under Employment Opportunities > Documents > Employment Forms or the New Employee Onboarding form.
        b. Make an appointment with the District Technology Director to review Data Usage and Classroom Tools

2. Read and sign the **Attalla City Schools Student Data Confidentiality Agreement.**

3. Once the above has been completed and forms reviewed, if all requirements are met, the new accounts will be enabled.

**Account will be created once the Technology Department receives the approved board agenda that lists new hires, roles, and work locations.

Forms

Student Data Confidentiality Agreement

I acknowledge my responsibility to respect the confidentiality of student records and to act in a professional manner in the handling of student performance data. I will ensure that confidential data, including data on individual students, is not created, collected, stored, maintained, or disseminated in violation of state and federal laws.

Furthermore, I agree to the following guidelines regarding the appropriate use of student data collected by myself or made available to me from other school/system employees, iNow, SETS or any other file or application I have access to:

A. I will comply with school district, state and federal confidentiality laws, including the state Data and Information Governance and Use Policy, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99; and, and the Attalla City Schools Student Data Confidentiality Agreement.
B. Student data will only be accessed for students for whom I have a legitimate educational interest and will be used for the sole purpose of improving student achievement.
C. I understand that student specific data is never to be transmitted via e-mail or as an e-mail attachment unless the file is encrypted and/or password protected.
D. I understand that it is illegal for a student to have access to another student's data. I will not share any student's information from any source with another student.
E. I will securely log in and out of the programs that store student specific data. I will not share my password. Any documents I create containing student specific data will be stored securely within the District network or within a password protected environment. I will not store student specific data on any personal computer and/or external devices that are not password protected. (external devices include but are not limited to USB/Thumb drives and external hard drives)
F. Regardless of its format, I will treat all information with respect for student privacy. I will not leave student data in any form accessible or unattended, including information on a computer display.

By signing below, I acknowledge, understand and agree to accept all terms and conditions of the Attalla City Schools Student Data Confidentiality Agreement.

_____ _____

Signature of Employee Date

_____ _____

Job Title School/Location