MCSS

Madison County School System



Data Governance Policies & Procedures

2023-2024

Madison County Board of Education, Approved March 23, 2023

MCSS
Madison County School System

Data Governance Policy & Procedures

MCBOE Approved 03.23.2023

TABLE OF CONTENTS

INTRODUCTION

DATA GOVERNANCE POLICY

- Scope 3
- Regulatory Compliance 3
- Risk Management 5
- Data Classification 6
- Systems and Information Control 6
- Compliance 10

APPENDIX A Definitions 11
APPENDIX B Responsibilities 13
APPENDIX C Data Classification Levels 16
APPENDIX D Acquisition of Software Procedures 17
APPENDIX E Virus, Malware, Spyware, Phishing, and SPAM 18
APPENDIX F Physical and Security Controls 20
APPENDIX G Password Control Standards 21
APPENDIX H Purchasing and Disposal Procedures 22
APPENDIX I Memorandum of Agreement (MOA 23

RESOURCES

Resource I ALSDE State Monitoring Checklist 29
Resource II Record Disposition Requirements 30

INTRODUCTION

Protecting student and staff privacy is a priority and the Madison County School System (MCSS) is 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 MCSS Data Governance document includes information regarding the Data Governance Committee, Data Governance Policy and Procedure, applicable Appendices, and Supplemental Resources.

The policy formally outlines how operational and instructional activity shall be carried out to ensure Madison County School System data is accurate, accessible, consistent, and protected. This document establishes responsibility for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The Madison County School System Data Governance Policy and Procedure shall be a living document. Supporting information for the MCSS Data Governance document are delineated in the Appendices and Supplemental Resources. With Madison County Board of Education approval, the Data Governance Committee may modify information in the Appendices in response to changing needs. The Madison County School System Data Governance Policy and Procedure document will be available on the district's website.

Data Governance Committee

The Madison County School System Data Governance Committee consists of the Superintendent or his/her appointed designee, Chief Schools Finance Officer, Instructional Technology Specialist, Information Technology Security Specialist, and the Director of Information Technology who will also serve as the Information Security Officer (ISO).

Committee Meetings

The Data Governance Committee will meet annually in June. Additional meetings may be called as needed.

MCBOE DATA GOVERNANCE POLICY

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

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

The superintendent is authorized to develop procedures in compliance with the above stated laws, statutory, regulatory or contractual obligations, to maintain data and information security measures that 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 Madison County Schools' data and information, including but not limited to:

- Speech - spoken face to face, communicated by phone, or any current/future technologies,
- Hard Copy Data - printed or written,
- Written Communications - sent by post/courier, fax, electronic mail, text, chat or any form of social media, etc.,
- Stored Data - processed by servers, PC's, laptops, tablets, or mobile devices, etc.
- Removable Storage Devices - internal, external, removable media or cloud based services.

Data Governance Procedures

Purpose

It is the policy of Madison County School System that data or information in all its forms- written, electronic, or printed- are protected from accidental or intentional unauthorized modification, destruction or disclosure. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.

- The Data Governance Policies and Procedure are reviewed annually by the Data Governance Committee.

- Madison County School System conducts annual training on data governance policy and documents that training.

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 may have access to district data systems or data. This policy applies to all forms of MCSS data and information, including but not limited to:

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

The intent of these procedures is to implement the laws governing the confidentiality of the school system's records. Nothing in these procedures is intended to create or expand any entitlement to the confidentiality of records beyond that which is established by law.

Furthermore, nothing herein should be deemed to create or expand any entitlement to copies of such records beyond what is established by law. In general, the Madison County School System reserves the right to adopt, revise, interpret, amend, repeal, suspend, or apply its policies and procedures according to its assessment of the needs and interests of the school system, subject only to such limitations on the exercise of such prerogatives as may be imposed by law.

Regulatory Compliance

The Madison County School System will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. The district's data governance policy and procedures are informed by the following laws, rules, and standards, among others:

Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA) 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: ***Children's Internet Protection Act (CIPA) | Federal Communications Commission***

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA)regulates organizations that collect or store information about children under the age of thirteen (13). Parental permission is required to gather certain information; see www.coppa.org for details.

For more information: ***Children's Online Privacy Protection Rule ("COPPA") | Federal Trade Commission***

Family Educational Rights and Privacy Act (FERPA)

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

For more information:***Family Educational Rights and Privacy Act (FERPA)***

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) 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. *In general, schools are not bound by HIPAA guidelines.*

For more information: ***HIPAA Home | HHS.gov***

Alabama Records Disposition Authority

Alabama Law Section 41-13-23 authorized the Alabama Department of Archives and History to publish rules for Local Government Records Destruction.

For more information, visit this link: http://www.archives.alabama.gov/officials/localrda.html

Protection of Pupil Rights Amendment (PPRA)

The Protection of Pupil Rights Amendment (PPRA) 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.

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

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

- Any other protected information survey, regardless of funding
- 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, and scoliosis screenings, or any physical exam or screening permitted or required under state law
- 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: What is the Protection of Pupil Rights Amendment (PPRA)?

Payment Card Industry Data Security Standard (PCI DSS)

This 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. See www.PCI security standards.org for more information.

For more information, visit this link: www.pcisecuritystandards.org

ISO Standards

- ISO 17799:2000 – Information technology – Code of practice for information security management.

- ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
- ISO 27002L2013 - Information technology – Security techniques – Code of practice for information security control

For more information, visit this link: http://www.iso.org/iso/home/standards.html

Risk Management

A thorough analysis of all Madison County School System information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or man-made, electronic and non-electronic – that affect the ability to manage the school system's information resources. The analysis will also document the existing vulnerabilities within each component of the information network and systems that could potentially expose school system data to threats.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the discretion of the person responsible for the component of the information network and systems in question.

The superintendent or designee will administer periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

Refer to Appendix B Information Risk Management Practices
Refer to Appendix C Definitions and Responsibilities

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.

Refer to Appendix D Data Classification Levels

Systems And Information Control

All 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 the Madison County School System shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

Ownership of Software

All computer software developed by Madison County School System employees or contract personnel on behalf of the district, licensed or purchased for MCSS use is the property of Madison County School System and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Software Installation and Use

All software packages that reside on technological systems within or used by Madison County School System shall comply with applicable licensing agreements and restrictions and shall comply with Madison County School System's acquisition of software procedures.

Refer to Appendix E Acquisition of Software Procedures

Virus, Malware, Spyware, Phishing and SPAM Protection

Virus checking systems approved by the MCSS Information 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 are not authorized to turn off or disable any security protection systems or to install other systems.

Refer to Appendix F Virus, Malware, Spyware, Phishing and SPAM Protection

Access Controls

Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the Data Governance Committee and approved by Madison County School System. 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 and Internal information and computing resources include, but are not limited to, the following methods:

- **Authorization:** Access to information systems will be granted on a case by case basis in order to fulfill a specific job responsibility. This access shall be authorized by the Information Security Officer with the assistance of the immediate supervisor.
- **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.

- The user must secure his/her authentication control (e.g. password token) such that it is known only to that user and possibly a designated security manager.

Data Integrity

Madison County Schools provides safeguards so that PII, Confidential, and Internal Information is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery.

In addition, listed below are methods that are used for data integrity in various circumstances:

- transaction audit
- disk redundancy (RAID)
- ECC (Error Correcting Memory)
- checksums (file integrity)
- data encryption
- data wipes

Transmission Security

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

- integrity controls and
- encryption, where deemed appropriate

Remote Access

Access into the Madison County School System's network from outside will be granted using MCSS approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PII, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protection as information stored and accessed within the MCSS network.

Physical and Electronic Access and Security

Access to areas in which information processing is carried out shall be restricted to appropriately authorized individuals. At a minimum, staff passwords shall be changed periodically.

- 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.
- Users must not leave any devices logged in, unattended, and accessible to unauthorized use.

Refer to Appendix G Physical and Security Controls Procedures
Refer to Appendix H Password Control Standards
Refer to Appendix I Purchasing and Disposal Procedures

Data Transfer/Exchange/Printing

- **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems shall be strictly controlled.

- **Internal Requests:** Any internal request from within the school system for a mass download of data that includes PII for research or any other purposes must be in accordance with this policy and be approved by the data governance committee.

- **External Requests:** Any external request from outside the school system for a mass download of the school system's electronic records must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. A memorandum of Agreements (MOA) or contract must 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 an exception is approved by the data governance committee. The contents of the MOA or contract will vary depending on the reason for the transfer and how the data will be used.

The school system may also release de-identified records and information for purposes such as research, provided that all personally identifiable information is removed and a reasonable determination is made that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. Such releases should be approved by the data governance committee.

Refer to Appendix J Madison County School System Memorandum of Agreement

Other Electronic Data Transfers and Printing

PII, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information must 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.

Oral Communications

Madison County School System 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. MCSS staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

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, procedures must be implemented to regularly review records of information system activity, such as audit logs, access report, and security incident tracking reports.

Evaluation

Madison County School System 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.

IT Disaster Recovery

Controls must ensure that the Madison County School System 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 and the Director of Information Technology 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:

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

American Disabilities Act (ADA)

The Madison County School System is committed to ensuring accessibility of its district and school websites for all students, parents, and members of the community, including those with disabilities and users of assistive technology. The Madison County School System continues to review and update its website to ensure compliance with current and future standards.

The MCSS website is required to be in compliance with Section 504 and Section 508 and Title II of the Rehabilitation Act. Section 504 requires equal access and communication of electronic information and data so that it is accessible to people with disabilities.

MCSS uses the Blackboard Web Community Manager to ensure that all website content or functionality on the district's websites will conform to the Web Content Accessibility Guidelines ("WCAG") 2.0, Level AA standards. This site has been built using code compliant with WCAG 2.0

Level AA standards for HTML and CSS. The site displays correctly in current browsers and using standards-compliant HTML/CSS code means any future browsers will also display it correctly.

The Blackboard Web Community Manager platform approaches accessibility in the following ways:

- Template-based pages and apps provide consistent interactions and user experience across pages.
- It allows clients to configure their templates while still remaining within the color contrast ratio.
- Provides full support for keyboard navigation.
- Text can be resized by 200 percent without loss of content or functionality.
- Contains page titles with the name of the workspace within which the user is working.

The district's website includes a variety of accessibility features including

- **Google Language Translation** tool on every MCSS webpage. This tool is located in the top left-hand corner of every webpage.
- **Alternate text- text-based** descriptions for images/graphics- unless they are decorative in nature.
- **Closed captioning** for video content through YouTube.
- **Logical tabbing sequence** for keyboard-driven navigation.
- **High color contrast** option- button to access this feature is at the top of every MCSS website.

If you would like additional assistance or are unable to access content on the dstrict's website, please complete our online **Website Feedback form**. You may also email mcss@mcssk12.org for assistance. Please include your full name, description of the problem encountered, the web address of the material you tried to access, and contact information in case more details are needed (email and phone number).

Website

The Madison County School System maintains and operates websites for the district and each school. The official website for the Madison County School System is www.mcssk12.org. Individual schools also have official websites through the district site.

The district web manager will be responsible for developing and overseeing all websites with the assistance of school-level web managers.

- No personal websites may be used to represent a school or class.
- No personal websites (including Google Sites) may be used to provide educational information to students and parents
- No personal websites may display school district or individual school names, logos, or other trademarks without permission.

- Booster clubs and organizations that support MCSS schools are not allowed to display school district or individual school names, logos, or other trademarks without express written permission from the superintendent. These organizations may utilize similar colors and designs to reflect a connection to a specific school or the district, but reproduction of protected branding is prohibited.
- Due to accessibility concerns, linking directly to external websites, those outside the district's management, is prohibited. Permission must be obtained from the MCSS Communications Department for exceptions to this procedure.

Compliance

The Data Governance Policy applies to all users of Madison County School System 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 MCSS 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 MCSS policies. Further, penalties associated with state and federal laws may apply.

The Madison County School System will conduct training on its data governance policy for employees, staff, volunteers, and outside affiliates that have responsibilities that include creating, using, or maintaining data as necessary and will maintain documentation of such training.

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

- Unauthorized disclosure of PII or Confidential Information.
- Unauthorized disclosure of a log-in code (User ID and password).
- An attempt to obtain a log-in code or password that belongs to another person.
- An attempt to use another person's log-in code or password.
- 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.
- Installation or use of unlicensed software on Madison County Schools technological systems.
- The intentional unauthorized altering, destruction, or disposal of Madison County Schools' information, data and/or systems. This includes the unauthorized removal from MCBOE 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.
- 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

Appendix A

Definitions

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Data: Facts or information

Entity: Organization such as school system, school, department or in some cases business

Information: Knowledge that you get about something or someone; facts or details.

Data Integrity: Data or information has not been altered or destroyed in an unauthorized manner

Involved Persons: Every user of Involved Systems (see below) at Madison County Schools – no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.

Systems: All data-involved computer equipment/devices and network systems that are operated within or by the Madison County 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.

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.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

Appendix B

Responsibilities

Data Governance Committee

The Data Governance Committee for Madison County 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 manage owners and users with comprehensive information about security controls affecting system users and application systems.

Information Security Officer

The Information Security Officer (ISO) for Madison County 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.
   Refer to 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 Madison County Schools Data Governance Committee on Madison County Schools' status with regard to information security.

User Management

MCSS 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. nitiating 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 Madison County 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.

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 submitting a request in writing to the Data Governance Committee for approval.

The owner of information has the responsibility for:

- Knowing the information for which she/he is responsible.
- 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.
- Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.
- Authorizing access and assigning data custodianship if applicable.
- Specifying controls and communicating the control requirements to the data custodian and users of the information.
- Reporting promptly to the ISO the loss or misuse of Madison County Schools' data.
- Initiating corrective actions when problems are identified.
- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- 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.

Data Custodian

The data custodian is assigned by an administrator, data owner, or the ISO based 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:

- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.

- 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.
- Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO and/or Data Governance Committee.
- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- Reporting promptly to the ISO and/or Data Governance Committee the loss or misuse of MCSS data
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified

User

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

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

Appendix C

Data Classification Levels

Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

- 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.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

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 Madison County Schools.

Confidential Information

- 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.

- Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Madison County 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.

Internal Information

Internal Information is intended for unrestricted use within Madison County Schools, and in some cases within affiliated organizations such as Madison County Schools’ business or community partners. This type of information is already widely-distributed within Madison County 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.

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

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

Public Information

- Public Information has been specifically approved for public release by a designated authority within each entity of Madison County Schools. Examples of Public Information may include marketing brochures and material posted to Madison County School System web pages.
- This information may be disclosed outside of the Madison County School System.

Directory Information

The Madison County School System defines Directory information as follows:

- Student first and last name
- Student home address
- Student home telephone number
- Student place and date of birth
- Student dates of attendance (years)
- Student grade level
- Student diplomas, honors, awards received
- Student participation in school activities or school sports
- Student weight and height for members of school athletic teams
- Student most recent institution/school attended

Appendix D

Acquisition of Software Procedures

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 Madison County Schools (MCBOE) as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

Software Licensing

All district software licenses owned by MCBOE will be:

- Kept on file at the central office,
- Accurate, up to date, and adequate, and
- In compliance with all copyright laws and regulations

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

Software installed on MCBOE 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 MCBOE employee purchasing and installing to ensure proper licensing

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:

- MCBOE student and/or staff data will not be shared, sold, or mined with or by a third party,
- MCBOE student and/or staff data will not be stored on servers outside the US unless otherwise approved by the MCSS Data Governance Committee,
- The company will comply with MCBOE guidelines for data transfer or destruction when contractual agreement is terminated, and
- No Application Programming Interface (API) will be implemented without full consent of MCBOE and the ALSDE.

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.

Supported Software

In an attempt to prevent software containing malware, viruses, or other security risk, 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 Coordinator, or their assigned designee(s).

1. A list of supported software will be maintained on the MCBOE District Technology site.
2. It is the responsibility of the MCBOE 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 MCBOE owned devices.
4. When staff recommends apps for the MCBOE 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 instructional 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 Coordinator and is therefore supported.

New Software

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

Evaluation may include but is not limited to the following:

- Conducting beta testing.
- Determining how the software will impact the MCBOE 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.

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.

When staff recommends apps for the MCBOE 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 is instructional sound, is in line with curriculum or behavioral standards, and is age appropriate.

Appendix E

Virus, Malware, Spyware, Phishing, and SPAM Protection

MCSS desktops, laptops, and fileservers run Anti-Virus software.

Internet Filtering

Student learning using online content and social collaboration continues to increase. The Madison County School System 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 district's content filter using the user's network credentials. This process sets the filtering level appropriately based on the role of the user, such as, student, staff or guest, and more specifically for students, the grade level of the child. All sites that are known for malicious software, phishing, spyware, etc. are blocked. Requests for blocking or unblocking may be submitted to the District Technology Coordinator, or his/her assigned designee. It is the responsibility of the requesting party to properly vet the site to ensure that is instructional sound, is in line with curriculum or behavioral standards, and is age appropriate.

Phishing and SPAM Protection

In addition to the built in spam filtering for Microsoft Exchange, email is filtered for viruses, phishing, spam, and spoofing.

Security Patches

Windows security patches and other Windows patches are scheduled to "auto-download" and "schedule install." Servers are scheduled to "auto-download" and are automatically updated.

Appendix F

Physical and Security Controls

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.

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.

Refer to Appendix I Purchasing and Disposal Procedures

Appendix G

Password Control Standards

The Madison County School System's Data Governance and Use Policy require 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 **Administration, Teachers, All Employees, Students.**

Password Standards

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

- Passwords shall never be shared with another person.
- Every password shall, where possible, be changed every 90 days, if not more frequently.
- Passwords shall, where possible, have a minimum length of eight (8) characters.
- When possible, for secure sites and/or software applications, user created passwords should adhere to the same criteria as required for network access.
- 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.
- Passwords shall not be programmed into a PC or recorded anywhere that someone may find and use them.
- 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.

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

- Passwords routed over a network shall be encrypted.
- Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- 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.
- 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.

Appendix H

Purchasing and Disposal Procedures

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 Madison County School System District Technology Coordinator.

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

Purchasing Guidelines

All systems that will be used in conjunction with MCSS technology resources or purchased, regardless of funding, shall be purchased from a list approved by the District Technology Coordinator. Systems not on the list must be approved by the District Technology Coordinator. 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. Also refer to the MCSS Computer Purchase Policy that was approved by the Board of Education, July 20, 2006.

Alabama Competitive Bid Laws

All electronic equipment is subject to Alabama competitive bid laws. Generally for technological devices and services, Madison County 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 the agreement, Madison County 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. See the Madison County Board of Education's Purchasing Policy.

Inventory

All technological devices or systems are inventoried in accordance with the MCSS Finance Department's policies. 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, fileservers, or district systems, etc. are inventoried.

Disposal Guidelines

Equipment shall be considered for disposal for the following reasons:

- End of useful life,
- Lack of continued need,

- Obsolescence,
- Wear, damage, or deterioration,
- Excessive cost of maintenance or repair.

The local school principal, District Technology Coordinator, and the Chief School 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 Business Office prior to the next Board of Education meeting:

- Fixed asset tag number,
- Location,
- Description,
- Serial number, and
- Original cost and account code if available.

Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to the Madison County School Board of Education Purchasing Policy, Chapter VII.

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 configured.

Discard

All electronic equipment in the Madison County 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 Madison County Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

Donation

All donations and/or sales shall be approved by the Madison County Board of Education.

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 MCBOE is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

MCBOE staff should make every effort before offering donated equipment, to make sure that it is in good condition and can be re-used. Microsoft licenses or any other software licenses are not transferred outside the Madison County School system.

Donations are prohibited to individuals outside of the school system or to current faculty, staff, or students of MCSS without Madison County Board of Education approval.

Required Documentation and Procedures

- For purchases, transfers and redistributions, donations, and disposal of technology-related equipment, it is the responsibility of the appropriate school staff member to create/update the inventory 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.
- When equipment is donated, documentation shall be on-file with the business office prior to the donation. Equipment is donated in order of request.
- 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.
- 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.
- 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 Finance Director 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.

Appendix I

MCSS Technological Services and Systems
Memorandum of Agreement (MOA)

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 MADISON COUNTY BOARD OF EDUCATION(MCBOE), 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 MCBOE Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all MCBOE 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 MCBOE Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all MCBOE Student Information. The Company shall take all reasonable steps to insure that no MCBOE Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for MCBOE under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of MCBOE, or (c) are entitled to such MCBOE student information from the Company pursuant to federal and/or Alabama law. The Company shall use MCBOE 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 MCBOE 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 MCBOE 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 MCBOE 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 e-mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify MCBOE of planned system changes that may impact the security of MCBOE data; (g) return or destroy MCBOE data that exceed specified retention schedules; (h) notify MCBOE of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of MCBOE information to the previous business day. The Company should guarantee that MCBOE 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 MCBOE 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 MCBOE student information compromised by the breach; (c) return compromised MCBOE data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with MCBOE efforts to communicate to affected parties by providing MCBOE 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 MCBOE 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 MCBOE 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 MCBOE 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 MCBOE data of any kind, failure to follow security requirements and/or failure to safeguard MCBOE data. The Company’s compliance with the standards of this provision is subject to verification by MCBOE 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 organization be allowed access to said information.

Disposition of MCBOE 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 MCBOE student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to MCBOE 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 MCBOE 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 MCBOE 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]

MADISON COUNTY SCHOOLS

By:_____
Ken Kubik
Superintendent
Madison County School System

Resource I

ALSDE State Monitoring Checklist

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 governa 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 ar 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	

Resource II

Record Disposition Requirement

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 File