Data Security Policy

Current Policy: Adopted:

The Superintendent is authorized to establish, implement, and maintain data security measures. Procedures to be established include a method of establishing data security classifications, implementing procedural and electronic security controls, and maintaining records regarding security access. The data security measures will apply to Board employees and all Board operations. Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual, may result in appropriate disciplinary action, which may include a recommendation for termination and other legal action.

Dissemination of Data Governance Policy

The Marshall County Board of Education Data Security Policy is available to the public and all internal stakeholders via the District Policy Manual at www.marshallk12.org.

The detailed policies, provisions, and procedures that serve to implement that Policy xxxx are shown below. As exposing these specific security measures to outside, unknown parties could result in greater risk to the District’s data, this document will not be made publicly available. Requests for detailed information about the District’s data security procedures shall be brought to the committee or the Superintendent who will determine the legitimacy of the request and respond accordingly.

Data Governance Committee

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charlie Jimmerson, Technology Coordinator</td>
</tr>
<tr>
<td>Janna Bonds, Data Manager</td>
</tr>
<tr>
<td>Laura Smith, CFO</td>
</tr>
<tr>
<td>Casey Partain, Child Nutrition Program Director</td>
</tr>
<tr>
<td>Brian Edmonds, Brindlee Mountain Middle School Teacher</td>
</tr>
<tr>
<td>Erica Stewart, DAR Middle School Librarian</td>
</tr>
<tr>
<td>Carla Thornton, Brindlee Mountain High School Registrar</td>
</tr>
</tbody>
</table>
Data Security Measures

I. Purpose

(A) Implement standards and procedures to effectively manage and provide necessary access to System Data, while at the same time ensuring the confidentiality, integrity and availability of the information. Insofar as this policy deals with access to Marshall County Schools’ computing and network resources, all relevant provisions in the Acceptable Use Policies are applicable.

(B) Provide a structured and consistent process for employees to obtain necessary data access for conducting Marshall County Schools operations.

(C) Define data classification and related safeguards. Applicable federal and state statutes and regulations that guarantee either protection or accessibility of System records will be used in the classification process.

(D) Provide a list of relevant considerations for System personnel responsible for purchasing or subscribing to software that will utilize and/or expose System Data.

(E) Establish the relevant mechanisms for delegating authority to accommodate this process at the school level while adhering to separation of duties and other best practices.

II. Scope

(A) These Security Measures apply to information found in or converted to a digital format. (The same information may exist in paper format for which the same local policies, state laws, statutes, and federal laws would apply, but no electronic control measures are needed.)

(B) Security Measures apply to all employees, contract workers, volunteers, and visitors of the Marshall County Schools and all data used to conduct operations of the System.

(C) Security Measures do not address public access to data as specified in the Alabama Open Records Act.

(D) Security Measures apply to System Data accessed from any location; internal, external, or remote.

(E) Security Measures apply to the transfer of any System Data outside the System for any purpose.
III. Guiding Principles

(A) Inquiry-type access to official System Data will be as open as possible to individuals who require access in the performance of System operations without violating local Board, legal, Federal, or State restrictions.

(B) The Superintendent and/or his designees shall determine appropriate access permissions based on local policies, applicable laws, best practices, and the Alabama Open Records Act.

(C) Data Users granted “create” and/or “update” privileges are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the System Data they create, update, and/or delete.

(D) Any individual granted access to System Data is responsible for the ethical usage of that data. Access will be used only in accordance with the authority delegated to the individual to conduct Marshall County Schools operations.

(E) It is the express responsibility of authorized users to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(F) These Security Measures apply to System data regardless of location. Users who transfer or transport System data “off-campus” for any reason must ensure that they are able to comply with all data security measures prior to transporting or transferring the data.

IV. Access Coordination

(A) Central Office Department heads, supervisors, area specialists, and principals (Authorized Requestors) will assist in classifying data sensitivity levels for their areas of expertise and in identifying which employees require access to which information in order to complete their duties.

(B) The System Technology Coordinator and Technical Services Supervisor will designate individuals within the technology department to implement, monitor, and safeguard access to System Data based on the restrictions and permissions determined by the Authorized Requestors using the technical tools available.

(C) Central Office Department heads, supervisors, area specialists, and principals will be responsible for educating all employees under their supervision of their responsibilities associated with System Data security.
V. Data Classification

(A) Marshall County Schools System Data shall be classified into three major classifications as defined in this section. Requests for changes to the established data sensitivity classification or individual permissions shall come from the above identified Authorized Requestors to the Technology Department.

1) Class I – Public Use
   This information is targeted for general public use. Examples include Internet website content for general viewing and press releases.

2) Class II – Internal Use
   Non-Sensitive (See Class III) information not targeted for general public use.

3) Class III – Sensitive
   This information is considered private and must be guarded from unauthorized disclosure; unauthorized exposure of this information could contribute to identity theft, financial fraud, breach of contract and/or legal specification, and/or violate State and/or Federal laws.

(B) FERPA Directory Information
   Information disclosed as ‘directory information’ may fall into either Class I or Class II, depending on the purpose of the disclosure. The following is the District’s list of which student information is to be considered ‘directory information’.

Marshall County Schools FERPA Directory Information Disclosure

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Marshall County Schools (District), with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child’s education records. However, Marshall County Schools may disclose appropriately designated ‘directory information’ without written consent, unless you have advised the district to the contrary in accordance with District procedures. The primary purpose of directory information is to allow the Marshall County Schools to include this type of information from your child’s education records in certain school publications. Publications may be in print or digital format. Examples include, but are not limited to, the following:

- A playbill, showing your student’s role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
• Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent’s prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks, take school pictures, or process data.

In addition, two federal laws require local educational agencies (LEAS) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, and institutions of higher learning, upon request, with three directory information categories – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student’s information disclosed without their prior written consent.

If you do not want Marshall County Schools to disclose ‘directory information’ from your child’s education records without your prior written consent, you must notify the school principal in writing within five (5) school days of the student’s first day of attendance.

The District may disclose the following information as directory information:
• Student’s name
• Address
• Telephone listing
• Electronic mail address
• Photograph
• Date and place of birth
• Major field of study
• Dates of attendance
• Grade level
• Participation in officially recognized activities and sports
• Weight and height of members of athletic teams
• Degrees, honors, and awards received
• The most recent educational agency or institution attended
• A student number assigned by the District (in some cases*)

* In order to make certain software applications available to students and parents, the District may need to upload specific ‘directory information’ to the software provider in order to create distinct accounts for students and/or parents. Examples of these include, but are not limited to MyLunchMoney.com, Blackboard Connect, and various education software applications. In these cases, the District will provide only the minimum amount of ‘directory information’ necessary for the student or parent to successfully use the software service.

VI. Compliance

(A) Data Users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to Class III (Sensitive) data; and to
abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure, or distribution of System Data in any medium is expressly forbidden; as is the access or use of any System Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

(B) Each employee at the System will be responsible for being familiar with the System’s Data Security Policy and these Security Measures as they relate to his or her position and job duties. It is the express responsibility of Authorized Users and their respective supervisors to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(C) Employees, whether or not they are Authorized Users, are expressly prohibited from installing any program or granting any access within any program to Class III without notifying the Technology Department.

(D) Violations of these Data Security Measures may result in loss of data access privileges, administrative actions, and/or personal civil and/or criminal liability.

VII. Implementation of Network/Workstation Controls and Protections and Physical Security

(A) Shared Responsibilities

1) The Technology Department shall implement, maintain, and monitor technical access controls and protections for the data stored on the System’s network.

2) System employees, including Authorized Requestors, shall not select or purchase software programs that will utilize or expose Class III data without first consulting the Technology Department to determine whether or not adequate controls are available within the application to protect that data. (The exception to this would be any software program purchased or utilized by the Alabama State Department of Education. In this case, the Alabama State Department of Education shall take all security responsibility for data it accesses or receives from Marshall County Schools.)

3) The Technology Department staff and/or the Authorized Requestor will provide professional development and instructions for Authorized Users on how to properly access data to which they have rights, when necessary. However, ensuring that all employees have these instructions will be the shared responsibility of the supervisor(s) of the Authorized User(s) and the Technology Department.

4) Technical controls and monitoring cannot ensure with 100% certainty that no unauthorized access occurs. For instance, a properly Authorized User leaves their workstation while logged in, and an unauthorized person views the data in their
absence. Therefore, it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.

(B) Authorized Requestors

1) Authorized Requestors (Section IV. A) are responsible for being knowledgeable in all policies, laws, rules, and best practices relative to the data for which they are granting access; including, but not limited to FERPA, HIPAA, etc.

2) Authorized Requestors shall be responsible for informing appropriate Technology Department personnel about data classifications in order that the Technology Department can determine the best physical and/or logical controls available to protect the data. This shall include:
   a. Which data should be classified as Class III
   b. Where that data resides (which software program(s) and servers)
   c. Who should have access to that data (Authorized Users)
   d. What level of control the Authorized User should have to that data (i.e. read only, read/write, print, etc.)

(C) Location of Data and Physical Security

1) Class III data shall be stored on servers/computers which are subject to network/workstation controls and permissions. It shall not be stored on portable media that cannot be subjected to password, encryption, or other protections.

2) Serving devices (servers) storing sensitive information shall be operated by professional network system administrators, in compliance with all Technology Department security and administration standards and policies, and shall remain under the oversight of Technology Department supervisors.

3) Persons who must take data out of the protected network environment (transport data on a laptop, etc.) must have the permission of their supervisor prior to doing so. Permission to do so will be granted only when absolutely necessary, and the person transporting the data will be responsible for the security of that data, including theft or accidental loss.

4) All servers containing system data will be located in secured areas with limited access. At the school or other local building level, the principal or other location supervisor will ensure limited, appropriate access to these physically secured areas.

5) District staff who must print reports that contain Class II or III data shall take responsibility for keeping this material in a secure location – vault, locked file cabinet, etc. In addition, all printed material containing Class III documentation shall be shredded when no longer in use.
(D) Disposal of Hardware containing System Data

1) Prior to disposal of any computer, the user will notify the Technology Department. A technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.

2) All schools and departments which purchase or lease copy machines or multifunction printers will be expected to include provisions for the destruction of data on the device’s hard drive or the destruction of the hard drive itself prior to disposing of the copier or MFP or its return the leasing agency.

(E) Application of Network and Computer Access Permissions

1) The Technology Department staff shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage, and access to all storage and transport mediums; including, but not limited to:
   a. Maintaining firewall protection access to the network and/or workstations.
   b. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing ‘guest’ wireless networks with limited network permissions.
   c. Implementing virus and malware security measures throughout the network and on all portable computers.
   d. Applying all appropriate security patches.
   e. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

2) Technology Department staff will apply protection measures based on the Data Classifications (see sections IV and V), including:
   a. Categorizing and/or re-classifying data elements and views.
   b. Granting selective access to System Data.
   c. Documenting any deviation from mandatory requirements and implementing adequate compensating control(s).
   d. Conducting periodic access control assessments of any sensitive information devices or services.

(F) Sensitive Data as it pertains to Desktops/Laptops/Workstations/Mobile Devices
1) Firewalls and anti-virus software must be installed on all desktops, laptops and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner.

2) Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers is prohibited, unless such information is encrypted in a Technology Department-approved encryption format.

3) The user responsible for the device shall take proper care to isolate and protect files containing sensitive information from inadvertent or unauthorized access.

4) Assistance with securing sensitive information may be obtained from school-level Technology Coordinators with input from the Technology Department, as necessary.

VIII. Transfer of Data to External Service Provider

(A) Student Class I data, directory information, and, in some cases Class II data, may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes. Provide that:

1) The teacher follows the protocols for getting approval for the site to be used.

2) The District notifies parents about their right to restrict their child’s data from being shared with such sites annually via Code of Conduct/AUP.

3) The transfer of data is handled in a manner approved by the Technology Department, or is performed by the Technology Department.

(B) No Class III data, or FERPA protected educational records, will be transferred to an external service provider without prior approval of the Data Governance committee. Exception: Alabama State Department of Education.

(C) No school or department should enter into a contract for the use of any program that requires the import of District data without first consulting and receiving approval from the Data Governance committee.

(D) The Data Governance committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:

1) Contract
2) Designating the service provider as an “Official” as defined in FERPA
3) Memorandum of Understanding
4) Memorandum of Agreement
5) Non-Disclosure Agreement
The following instructions comply with Marshall County Schools Policy xxx Data Security

When to Use a Non-Disclosure Agreement

1. **Private Information.** Confidential information, as defined by FERPA and other regulations and policies, is to be protected and disclosed only to those employees who have a direct legitimate reason for access to the data in order to provide educational services to the student.

2. You must seek guidance from the Student Services, Special Education, and/or the Technology Department prior to transferring confidential information to any outside company, online service (free websites), or to any outside individual, organization, or agency without the explicit written permission of the parent of a minor student or an adult-aged student. This information includes:

   1) Social Security number
   2) Grades and test scores (local and standardized)
   3) Special education information
   4) Health information and 504 information
   5) Attendance information (not enrollment, but specific attendance dates)
   6) Family/homeless/or other similar status
   7) Child Nutrition Program status (free or reduced meals)

This includes providing confidential information to individuals, including System employees, for use in dissertations or other studies for college courses or doctoral studies. Refer all such requests, including those for federal, state, or other studies to the Instruction Department and the Technology Department for their approval before releasing any such individualized information. Approved recipients may be required to complete an NDA so that they fully understand their responsibilities with regard to safeguarding and later destroying this private information. This restriction does not apply to publicly available **aggregated** data such as dropout rates, attendance rates, percentage of free and reduced lunch program students.

Exceptions. Other Public K-12 Schools - Private information may be transferred upon request to the State Department of Education or other public school systems with a legitimate need for the data; however, the transfer process should comply with data security protocols (see below). In addition, personnel must research all recipients to ensure that the school is legitimately a public school rather than a private school.

Colleges – Confidential information may be transferred to institutions of higher education, when the adult student or the parent of a minor student requests that transcripts or other private information be released to specific institutions. Such information should not be transferred to colleges based on a request from the college directly, unless approved by the individual whose records will be transferred.

3. **Directory Information.** Although Marshall County Schools has identified the following as “Directory Information,” schools should still carefully consider the transfer or publication of this information. Seek guidance when in doubt. Much of this information, combined with data collected elsewhere can be used for identity theft purposes, stalking, and other unlawful or unethical purposes.

   1) Home address
   2) Home or cell phone numbers of students or their parents
3) Email addresses of students or their parents
4) Date and place of birth

Exception: U.S. Military and institutions of higher learning for recruiting purposes. However, school must first determine which parents have submitted Opt Out forms relative to these requests prior to transferring data.

(E) Non-Disclosure Agreement Processing

1) The Technology Department will keep all NDAs on file. This will eliminate the need for each school to solicit an NDA from companies which already have NDAs on file. Technology will also ensure that the NDA is renewed annually where necessary.

2) What the school should do:
   a. Get the following specific information from the “entity” to which you want to transfer the information: company name, web address, phone number, fax number, and email address, name of individual you are working with.
   
   b. List the information you wish to transfer to the ‘entity’
   
   c. Send this information to the Technology Department for referral to the Data Governance Committee.

3) Upon approval by the Data Governance Committee, the Technology Department will determine if there is a current NDA already on file with the entity. If not, one will be prepared and sent to them. Once the agreement has been signed, the Technology Department will notify the school and oversee the process of securing uploading the necessary data to the service provider.

4) Note that all confidential data that will be transferred by email, whether in the body of the email or as an attached file, should be encrypted. The Technology Department can help you with transporting this data.

(F) Sample Non-Disclosure Agreement

Nondisclosure Agreement

THIS NONDISCLOSURE AGREEMENT (this “Agreement”), by and between Marshall COUNTY SCHOOLS, AL (the “District”), and ___________________ (the “Service Provider”), relates to the disclosure of valuable confidential information. The “District” refers to all schools, departments, and other entities within Marshall County Schools. The Service Provider refers to any free or fee-based company, organization, agency, or individual which is providing services to the District or is conducting District-approved academic research. The Disclosing Party and the Receiving Party are sometimes referred to herein, individually as a “Party” and collectively, as the “Parties.”

To further the goals of this Agreement, the Parties may disclose to each other, information that the Disclosing Party considers proprietary or confidential.
The disclosure of District’s Confidential Information by a Receiving Party may result in loss or damage to the District, its students, parents, employees, or other persons or operations. Accordingly, the Parties agree as follows:

Confidential Information disclosed under this Agreement by the District shall only be transmitted in compliance with the District’s approved security protocols. The Receiving Party must accept the data transmitted in these formats.

The Service Provider will request or receive Confidential Information from the District solely for the purpose of entering into or fulfilling its contractual obligations or pre-approved academic research.

The Service Provider agrees not to use, or assist anyone else to use, any portion or aspect of such Confidential Information for any other purpose, without the District’s prior written consent.

The Service Provider will carefully safeguard the District’s Confidential Information and may be required to describe such safety measures to the District upon request.

The Service Provider will not disclose any aspect or portion of such Confidential Information to any third party, without the District’s prior written consent.

Confidential Information disclosed under this Agreement shall not be installed, accessed or used on any computer, network, server or other electronic medium that is not the property of the District or the Service Provider, or to which third-parties have access, unless otherwise provided in a separate contract or agreement between the Parties hereto.

The Service Provider shall inform the District promptly if the Service Provider discovers that an employee, consultant, representative or other party, or any outside party has made, or is making or threatening to make, unauthorized use of Confidential Information.

The Service Provider shall immediately cease all use of any Confidential Information and return all media and documents containing or incorporating any such Confidential Information within five (5) days to the District after receiving written notice to do so, or whenever the contract for services between the District and the Service Provider expires or is terminated. In addition, the Service Provider may be required by the District to destroy any Confidential Information contained on primary or backup media upon written request of the District.

<table>
<thead>
<tr>
<th>Date</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>District</td>
<td>Service Provider</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Printed Name</th>
<th>Printed Name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
<th>Signature</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Title</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Phone/Email</th>
<th>Phone/Email</th>
</tr>
</thead>
</table>

Confidential Information includes:

- any written, electronic or tangible information provided by a Disclosing Party
- any information disclosed orally by a Disclosing Party that is treated as confidential when disclosed
- all information covered by FERPA or other local, state, or federal regulation applying to educational agencies
IX. Reporting Security Breaches

All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.

Data Governance Training

I. School and Central Office Administrators

(A) School and Central Office Administrators will receive refresher training on FERPA and other data security procedures annually at principals meetings

(B) Principals and Central Office Administrators shall contact the Technology Coordinator or the Students Services Department when in doubt about how to handle Class II and III information

(C) Principals and Central Office Administrators will be kept aware of emerging issues pertaining to data security, such as the information shown in Exhibit B.

II. School Registrar Data Security Training

(A) School registrars will be trained and refreshed on FERPA and other data security procedures twice annually.

(B) School registrars’ adherence to the data security procedures will be monitored by the Technology Department through random audits.

III. Teacher and Staff Training

(A) All new teachers will complete training on all District technology policies, including how their use of technology is governed by FERPA and other data security procedures established by the District.

(B) All department heads will be expected to educate their support staff on data governance as it applies to their department’s work.
(C) All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.

**IV. Parent and Booster Training**

(A) School administrators shall educate PTOs, boosters, and other parent groups about FERPA and student confidentiality. For instance, organizations who intend to post information about the school's students or activities should not compromise the privacy of students in protective custody. Because the school cannot tell these groups which students may be in such situations, the organization should be cautioned about exposing any information or photos that could cause harm to students or their families.

(B) The Technology Department shall have procedures that include educational materials for booster organizations who wish to post their own websites. This shall include both FERPA and COPPA information.

**Data Quality Controls**

**I. Job Descriptions**

(A) Job descriptions for employees whose responsibilities include entering, maintaining, or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality, and completeness. This includes, but is not limited to: school registrars, counselors, special education staff, and CNP staff handling free and reduced lunch data.

(B) Teachers shall have the responsibility to enter grades accurately and in a timely manner.

(C) School administrators shall have the responsibility to enter discipline information accurately and in a timely manner.

**II. Supervisory Responsibilities**

(A) It is the responsibility of all Supervisors to set expectations for data quality and to evaluate their staff’s performance relative to these expectations annually.

(B) Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department, including the State Department of Education, if applicable.
Student Information Systems

I. Student Information Applications

(A) Any software system owned or managed by the District which is used to store, process, or analyze student ‘educational records’ as defined by FERPA shall be subject to strict security measures. These systems are:

1) INOW – General student information system
2) SetsWeb – Special Education information system
3) WinSnap – Child nutrition information system

(B) Administrators with supervisory responsibilities over the District’s Student Information Systems shall determine the appropriate access rights to the data and enforce compliance with these roles and permissions.

II. INOW Access

INOW, unlike its predecessor STI Office, enables authorized users to access the application from anywhere they may have Internet access. In response to this anywhere/anytime access, as well as the fact that INOW provides less-granular permission settings than its predecessor, the Data Governance Committee and its, INOW permissions sub-committee, has implemented the following:

(A) Strong password requirement for INOW logins

(B) Data Security Agreements for those with INOW permissions who are not teachers

---

**STI Data Security Agreement**

Please read the document carefully and notice that it warns against removing personal data on students and employees from the workplace. This type of information should not be carried outside of your school on USB drives, disks, or on laptops. If any of these portable devices were to be lost or stolen, it could put the system at great risk.

Please make enough copies of this document for each of your staff who have STI Office permissions to sign. Have them sign the form. Make them a copy of the signed form, and then forward the original to the Technology Department. This will include you, your assistant principals, your counselors, the school nurse, and a few others in your school. The registrars have already received and signed a copy at the recent Registrar’s meeting.

If you have questions, please feel free to contact me.
Marshall County Schools Data Security Agreement

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one’s job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Marshall County Schools’ student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or district administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.

I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.

Please sign below to indicate you understand and agree to the above statements.

<table>
<thead>
<tr>
<th>Printed Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
</table>
Data Security Agreement: Athletic – Quick Entry Edit Provision

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one’s job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Marshall County Schools’ student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or district administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.

I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.

Athletic – Quick Entry Edit Provision

I understand that access to the Quick Entry Edit utility is being added to my permission so that I may rapidly identify student athletes per the directions provided by the AHSAA. I agree not to delegate this responsibility to others. I will be careful in selecting the Athletic field and the correct students so that school does not incur unintended insurance costs.

Please sign below to indicate you understand and agree to the above statements.

<table>
<thead>
<tr>
<th>Printed Name/Title</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(C) ‘Notification of Risks’ to school administrators and registrars

Notice of Risks Related to INOW Usage

**INOW Access for Parent Volunteers**
Some schools rely on parent volunteers to help greet visitors and locate students. Due to FERPA and other confidentiality expectations volunteers should only be granted very limited INOW rights. In most cases this should be the ‘Schedule Lookup’ level of access which enables the volunteer to see a list of all students and their schedules. Remember, INOW permissions are web-based so what volunteers can see from the school, they can also access from anywhere they have Internet access.

**Concerns about Parent Volunteers Checking Students Out of School**
Releasing a child from school into the care of someone else is a serious responsibility. Schools should carefully assess whether or not the information in INOW for this purpose is always up to date. In the past registrars have raised concerns that parents often change their minds about who can and cannot check out their children, but they don’t necessarily notify the school in a timely manner. This makes the prospect of allowing parent volunteers who are unfamiliar with the current circumstances of various family situations to check out students an area of concern.
Student Services will be providing recommendations regarding this important function.

**Allowing Others to Use Another User’s INOW Account to ‘Give’ them Greater Access is Prohibited**
A user’s INOW permission level is based on their job responsibilities. Violating FERPA can have serious consequences, including the loss of Federal Funding and other legal liabilities. Since we have a responsibility to protect our student and employee data from identity theft or other misuse, no one may log into INOW and allow others to use their access. Participating in this practice violates our Acceptable Use policies and Data Security Procedures.

The Technology Department will perform random scans to determine if the same INOW user id is in use concurrently on two separate computers and investigate these occurrences as warranted. Registrars who are using multiple machines have been instructed to notify Technology of this so that dual logins on specific IP addresses will not be viewed as a potential violation of this rule.

**Plan for when your Registrar is Out for an Extended Period**
You should have a plan for occasions when your registrar is out sick or on vacation. Anyone filling in for the registrar should be a bona fide employee, not a volunteer. Technology will attempt to help in extreme situations, but our ability to do so is limited.

**Providing Information to Others on Students NOT Enrolled at Your School**
INOW rights intentionally prevent the staff at one school from seeing information on students at another school, which complies with FERPA guidelines. The only exception is for district level personnel who have specific needs to see all school data and teachers or others who serve specific students in multiple schools.

It is important that staff members at one school do not attempt to give information about students enrolled in another school to individuals who ask for such information. Instead they should expect the person asking for the information to contact that school themselves. If the
person asking for information does not know what school to contact, then they should be referred to the Student Services Department.

DO NOT tell an individual who has no official right to know where else the student is enrolled. Even if the person asking is a parent, there may be a dangerous situation that you are now unaware of, so the safe action to take is to refer such requests to the Student Services Department.

The danger in telling someone, employee or not, what other school the child is enrolled in lies in the fact that you have no access to that student’s record and will not know if the child is in protective custody or is involved in some other situation such as custody dispute, etc. This could result in a safety issue.

This rule applies even when the person asking for the information is one of our own employees. Unless the person requesting the information is currently providing educational services to that student, they should not be given any information about them, including where the student is enrolled. And, if they are providing educational services to a student at another school, but claim not to know where the child is enrolled, then this should raise some flags. In this case, contact Student Services for guidance.

Data Backup and Retention Procedures

I. Purpose of Data Backup and Retention Procedures

(A) Ensure that procedures for comprehensive data backup are in place and that system data is restorable in the event of data corruption, software or hardware failures, data damage or deletion (either accidental or deliberate), and properly executed requests from the office of the Superintendent, or forensic purposes.

(B) Provide a documented policy of how long data is retained, and therefore restorable.

(C) Provide documentation of what systems and data are specifically included in, and excluded from, backup and retention.

(D) Establish the groups or individuals responsible for data backup and retention procedures, including the on-site and offsite locations of backup media.

(E) Establish the procedural guidelines used to initiate a data restore.
II. Scope

(A) This Policy applies to all servers and systems installed and controlled exclusively by the Marshall County Schools Technology Department. (Systems Table I) and excludes servers and systems controlled by specific departments within Marshall County Schools (Systems Table II). In cases where other Departments are responsible for their backup systems, the Technology Department will provide technical and professional guidance for backup routines and procedures, as requested.

(B) This Policy applies to all user data in the following manner:

All users with network permissions are trained and urged to store data onto their server workspace, but they are permitted to store files on local machines. Individuals users may delete their data from either network servers or local machines at will. If data stored on a server is deleted by the end user and falls outside of the backup period, the System has no method of recovering such files.

Files stored by users on individual hard drives or other individual storage devices are not backed up and may become unrecoverable in the case of hard drive failure or accidental deletion. Although technicians may be able to locate or recover locally stored files, these files are not part of the data backup or recovery plan.

(C) This Policy does not apply to connected systems which are the property, and therefore the responsibility, of outside entities such as the Alabama State Department of Education.

(D) This Policy includes a special section for the e-mail system, as its backup and retention system is separate from other systems.