Bullock County School District

Data Governance

The following documents are affiliated with Bullock County School District Data Governance policy, procedures, training, and guidance.

Contents

State Monitoring Checklist Cross-Reference

	ON-SITE	INDICATORS	SCS Data Governance Plan
1.	Has the 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	See committee files Committee
2.	Has the local school board adopted a data governance and use policy?	Copy of the adopted data governance and use policy Dated minutes of meetings and agenda	Board Policy
3.	Does the data governance policy address physical security?	Documented physical security measures	Controls and Protections
4.	Does the data governance policy address access controls and possible sanctions?	Current list of controls Employee policy with possible sanctions	General provisions Data transfers INOW Permissions Reporting breaches Data Security Agreements Email –Violations and Enforcement
5.	Does the data governance policy address data quality?	Procedures to ensure that data are accurate, complete, timely, and relevant	Quality Controls
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	Data transfers and Non-Disclosure Agreements Disclosure of data via email
7.	Has the data governance policy been documented and communicated in an open an 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	Dissemination of policy Data Security Training

7

Applicable Laws and Standards

The District 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:

FERPA

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

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: http://www.archives.alabama.gov/officials/localrda.html.

ALABAMA OPEN RECORDS LAW

COPPA

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

HIPAA

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

Data Security Policy

Policy History:

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.	

Data Governance Committee

Name	**Department**
Christopher Blair	Superintendent
Michael King	Special Education
Herbert McGowan, District Tech Coordinator	Technology Support Services

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 Bullock County School District' 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 Bullock County School District 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 Bullock County School District 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 Bullock County School District 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) Bullock County School District 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’.

Bullock County School District FERPA Directory Information Disclosure

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Bullock County School District, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, the Bullock County School District 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 Bullock County School District 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 Bullock County School District 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 the lunch program, Google Apps for Education, Bullock County Police Department, District Attorney’s Office, 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.

Data Classifications for Students

Student Data	Classification	Authorized Users	Web Access
Student Name*	Class I or II, depending on use	All, as needed	First Name, Last Initial only, except in press release, school newspaper, or C2C
District Student Number	Class II	Principal, Asst. Principal, Counselor, Registrar, Teachers, Student, Parent, CNP, Media Specialist. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
State Student Number*	Class II	Principal, Asst. Principal, Counselor, Registrar Student, Parent	No
Social Security Number*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker	No
Home Phone Number	Class I or II, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers. School directories with parental permission being first obtained. Rapid notification system directory.	No
Home Address	Class I, II, III, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers	No
Ethnicity*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers	No
National School Lunch Program Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, CNP Coordinator and staff, Immediate teacher, (Point of Sale transactions will be done in	No

		such a way as to not identify students who receive free or reduced lunches. Cafeteria managers and CNP employees who process F/R applications or lists of benefit recipients will ensure the information is secure and made available only those persons who require it.)	
ESL Status*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, ESL Supervisor, ESL Dept. employees, Assigned Teachers and After School Care workers	No
Special Ed Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers.	No
Medical Conditions	Class III, except in emergencies	Principal, Asst. Principal, Registrar, Nurse, Immediate Teacher, Lunch Room personnel (if food allergy), and After School Care workers, if applicable	No
Grades	Class III, except when used in conjunction with honor rolls/awards	Principal, Asst. Principal, Registrar Immediate Teachers, Student, Parents or legal guardian, School Counselor, Gifted Teacher (only for students assigned), PST Committees, Appropriate Central Office Administrators, Testing Coordinator, Transfer to schools and Scholarship applications, C2C	INOW Parent Portal - Access is to be given to parents or legal guardians only. INOW Teacher web access
Attendance*	Class III	Principal, Asst. Principal, Attendance Clerk, Registrar, Student Services Coordinator and staff, Truancy Officers, School Resource Officer, Immediate Teachers, PST Committee	INOW Parent Portal only
Discipline*	Class III	Principal, Asst. Principal, Counselor, SRO, Registrar, Student Services	No
Standardized Test Scores*	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, PST Committee, Student, Parent	No

System Benchmark Test Scores	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, PST Committee, Student, Parent	No
*ALSDE may access all such information for State Reporting Collection purposes			

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 Bullock County School District.)

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 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) **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.

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

3) 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

(E) Non-Disclosure Agreement (NDA) Information

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 doctorial 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 Bullock County School District 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 BULLOCK COUNTY SCHOOL DISTRICT, 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 Bullock County School District. 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.

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.

Date	Date
District	Service Provider
Printed Name	Printed Name
Signature	Signature
Title	Title
Phone/Email	Phone/Email

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 ● any other information not covered by FERPA, HIPAA, or other local, state, or federal regulation which the District requires the Service Provider to treat as confidential

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.

II. School Registrar Data Security Training

(A) School registrars will be trained and refreshed on FERPA and other data security procedures 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 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) MCS – Child nutrition information system
4) Compass Learning
5) ThinkCentral
6) Scholastic (Read 180/System 44)
7) School Messenger
8) Global Scholar
9) Edgenuity
10) Pearson SuccessNet
11) Atriuum
12) Renaissance Place
13) Fast Forward
14) Reading Assistance
15) AMSTI
16) ARI
17) DIBELS Next
18) Scantron
19) IB
20) Go Math
21) Reading Street
22) Stems Scope
23) Big Brainz
24) Coach Science
25) Coach-Buckledown
26) Edmentum
27) Fast Math
28) Imagine Learning
29) Infobase Learning
30) Ladders for Success
31) RAZ Kids
32) SRA
33) Studies Weekly
34) Teacher Created Material
35) Science In Motion
36) Science Learning
37) True North
38) ACT
39) American Heart Association
40) Certi Port
41) Copper Media
42) G Metrix
43) FEMA
44) Fiber Media
45) IC3
46) Measure UP
47) Microsoft
48) NCCER
49) Network Pro

50) Online Expert
51) PC Pro
52) ASPIRE
53) John Hopkins University
54) Math Science Partnership with Tuskegee University
55) SECME
56) TRIO (ASU)
57) AL Council Economic and Financial
58) AL Financial Literacy Challenge
59) Center of Science and Industry
60) Vision Makers
61) WISE Financial Literacy
62) Registration Gateway (SRC)
63) Guide K12
64) Blackboard
65) LeanFrog

(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) Password requirement for INOW logins

(B) 'Notification of Risks' to school personnel

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.

Financial Data

Please do not share your computer login with anyone. Your financial payroll data is available under the same account that you log onto computers and email with. Sharing your account information would potentially share this information as well.

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.

INOW Permission Standards for the Bullock County School District

I. Data Governance Committee

(A) Principals/supervisors must submit names to the Technology Department via work order and list the associated role from the list below.

(B) The data governance committee will meet annually in order to review permissions and to consider new requests. Requests that are made between annual meetings will be presented to the members via email or in-person, as appropriate. Changes will be conveyed to affected personnel via memos and updates to the manual. (See Exhibit A.)

II. Allowable INOW Permission Settings

Group: **Find Student Only** (Schedule Lookup)

Staff Affected: All INOW Users. (Parent Volunteers may be granted this permission, but only when the INOW Permissions Committee approves a request submitted by a principal.)

All INOW users can use the Look Up feature to find any student's current location. The staff can also refer to a Student Schedule Matrix pdf file which the school's Registrar will post to the Faculty Share. Registrars will update the file as needed.

Only Technology INOW administrators can add individuals to this permission group.

Group: **Check In/Out**

Staff Affected: Assigned by Technology upon request

This level of permission allows the user to see the Summary, Main, and Contacts tabs.
It gives them the ability to check students in and out and to view the following information:

- Name
- Date of Birth
- Age
- Phone (This can be hidden if necessary)
- Gender
- Grade (This can be hidden if necessary)
- Address (This can be hidden if necessary)
- List of Contacts and their relationship and phone numbers

The user will see the special symbols, but not open up these notes to see what instructions they contain.

Only Technology INOW administrators can add individuals to this permission group.

Group: **Limited Student View**

Staff Affected: Library Media Specialists*

Staff with "Limited Student View" permissions will have Read-Only rights to contact information for all students in the school.

**Library Media Specialist may have additional permissions if they give grades or serve in other roles within the school.*

Only Technology INOW administrators can add individuals to this permission group.

Group: **Test Data Entry**

Staff Affected: Secretaries in counseling offices (if requested by principal)

These permissions enable staff to enter testing data.

Only Technology INOW administrators can add individuals to this permission group.

Group: **Special Student View**

Staff Affected: Individuals serving in the following roles, when endorsed by the principal/supervisor

- Athletic Directors (Can also be added to AD Quick Entry Edit Group, see below)
- Lead Special Ed Teachers
- Lead ESL Teachers
- PST Chairperson

Staff with "Special Student View" permissions will be able to see the following information for ALL students in the school:

- Contacts – full records
- Grades which have been posted by teacher
- Attendance profile
- Schedules

Principals may also want to ask Registrars to set up Non-Reporting Class Rosters (see below) for individuals who have been granted Special Student View permissions. Or, they may want to request that these individuals be set up with Non-Reporting Class Rosters *instead of* being given the Special Student View. In either case, Non-Reporting Classes can make it easier for individuals to look up information on the students they are responsible for because it will enable them to check each student's information from a 'class' roster (i.e. football, PST, girl athletes, etc.) rather than look up each student by name in INOW. Creating these 'Non-Reporting Class Rosters' will take more work on the Registrar's part. However, it is a good option when principals want to restrict access to only the students served by the individual, rather than all students in the school.

Group: **Athletic Directors Quick Entry & Future Year**

Staff Affected: Athletic Directors only

Middle and high school athletic directors will be given the ability to use the Quick Entry Edit feature in INOW to edit students' eligibility settings, but only after being trained by the school registrar.

Athletic Directors with this permission must sign the associated Security Agreement.

Group: **Non-Reporting Class Rosters**

Staff Affected: Various

When teachers have a formal responsibility to support students who they do not have on a class roll, and this responsibility includes viewing the students' grades, then the Registrar may be asked to set up a Non-Reporting Class for that teacher. Examples of these situations/individuals include:

- Special Education teachers with students on their caseload, but who are not in their class
- Academics First Sponsor
- Math or Reading Coaches, where applicable
- Gifted advisors, where applicable
- Anyone who already has or would be eligible for the Special Student View (above)

Once the 'class' is created, the 'teacher' will have the ability to 'print' a comprehensive progress report for the students which will give the 'teacher' access to posted grades from all classes. Keep in mind that this will take some work on the Registrar's part. In the case of the Athletic Director and a separate Academics First teacher, they could both be listed as teachers for the non-reporting class to minimize the work involved.

The Technology Department will provide Registrars with directions for creating these non-reporting classes. These directions must be followed carefully so that the courses do not affect attendance, LEAPS, or other state reports. These courses will need to be scheduled outside of the school day, must be tagged as a non-reporting course in the Master Schedule, and must use the correct State Course Number.

Group: **Discipline History**

Staff Affected: Administrators Only

Only school administrators will have access to student discipline history. Staff should consult with their school administrators if they need discipline history on a given student.

AHSAA Student in Good Standing Forms –

The AHSAA Student in Good Standing Release Form must be completed and signed by the school Principal. This is only to be completed when the student athletes leaving your school are not in good standing.

I. INOW Substitute Teacher Set Up & Roles

All Subs and Temporary Employees who are granted INOW access must sign the STI Security Agreement and AUP. The school registrar should facilitate this and store the Agreement at the school. If a Long Term Sub works at more than one school, each school should have a signed Agreement on file.

When possible, the teacher going on leave should set up the class grade book before the Long Term Sub takes over. Technology INOW administrators can assist in setting up grade books if the teacher is not able to do so prior to his/her absence.

Group: **Substitute Teacher Access**
Staff Affected: Long Term Subs and Temporary Employees

Scenario 1: **Short Term Sub (under 21 days)**

INOW: No access

- If the teacher does not return after 20 days, then the sub may have INOW access as a Long Term Sub. Select the appropriate Scenario from those listed below.
- If it is known in advance that the teacher will be out for longer than 20 days but less than 1 semester then use either Scenario 2 or 3, whichever applies.

Scenario 2: Sub over 21 days, but less than 1 Semester (aka Long Term Sub)

INOW Role:	Long Term Sub
INOW Schedule:	Additional Teacher

Scenario 3: Long Term Sub/Temporary Employee* for more than 1 semester, but less than 1 year

INOW Role:	Long Term Sub
INOW Schedule:	Additional Teacher

EXCEPTION: If the original teacher will not be returning to your school (i.e. transferring, resigning, retiring, etc.) then they should be removed from the master schedule and the teacher replacing them should be shown as:

INOW Role:	Long Term Sub
INOW Schedule:	Teacher

Scenario 4: Temporary Employee* for one full year

If the ***original teacher has highest degree*** and years of experience, then the Temporary Employee will have:

INOW Role for Temporary Employee:	Long Term Sub
INOW Schedule for Temporary Employee:	Additional Teacher
INOW Role for Teacher on Leave:	First Primary Teacher
INOW Schedule for Teacher on Leave:	Teacher

If ***the temporary employee has highest degree*** and years of experience, then the Temporary Employee will have:

INOW Role:	First Primary Teacher
INOW Schedule:	Teacher
INOW Role for Teacher on Leave:	None
INOW Schedule for Teacher on Leave:	None

Email Use and Security Agreement

I. User Agreement

All individuals issued an email account by Bullock County School District are expected to follow the District's Email Use and Security Agreement. This agreement is provided all new staff.

II. Bullock County School District Email Disclaimer

This message, and any files transmitted with it, may contain confidential information and is intended only for the individual addressee(s). If you are not the named addressee or if you have received this email by mistake, you should not disseminate, print, distribute or copy this e-mail. If you have received this email by mistake, please notify the sender immediately and delete this e-mail from your system.

Data Backup and Retention Procedures

The following standards may be updated, amended, or changed as needed.

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.

II. Scope

(A) This Policy applies to all servers and systems installed and controlled exclusively by the Bullock County School District Technology Support Services. Data stored on individual school edservers is not backed up, nor covered under this policy.

(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 covered by backup 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.

III. INOW Alabama State Back Up

(A) Student Information System - Offsite Remote Backup

1) Currently INOW is hosted from the vendor offsite. We do not have to back up any information or perform any updates on our end.

IV. Email Archiving

(A) In October, 2014, a Barracuda Email Archive appliance was added to the network. The device is set to retain all internal and external mail for long-term retrieval purposes. The size of the hard drive space allotted for this may need to be expanded over time to accommodate a full year of data. Expansion of disk space will be based on available funding at the time. Prior to the addition of the Barracuda Email Archive appliance, the back-up/retention appliance was provided by InBoxer.

(B) The Barracuda Email Archive appliance is not backed up. Losses from catastrophic events damaging equipment or data may be irrevocable.

(C) Event Log for Email Archiving

V. Responsibility of Data Backup and Data Retention

(A) The Technology Department assumes responsibility of facilitating, operating, maintaining, checking and testing the backup system.

(E) The ultimate responsibility of the Backup system, maintenance, operation and procedures falls to the Technology Support Services Systems Administrators.

End of Document Backup and Retention Procedures

Exhibit C: Email User Agreement

Electronic communications, in its many forms, can be a very efficient and effective method of communicating with others; however, it has many inherent risks. Once sent or posted, the author no longer has control over the information contained in the message or posting. The purpose of this Acknowledgement is to make Bullock County School District employees and others granted network accounts aware of certain risks and responsibilities that accompany using electronic communications provided by Bullock County School District.

This Acknowledgement provides guidance on the professional, ethical, legal, and responsible use of System electronic communications (E-mail, list serve, web site, etc.). This document does not constitute all rules concerning electronic communications. Refer to Bullock County School District' Policy website for a complete list of policies.

This Acknowledgement applies to all full-time employees, part-time employees, contracted employees, temporary employees, and other agents operating on behalf of Bullock County School District. It applies to any person or group of persons who have E-mail accounts, and also to those who request that an account holder send a message on their behalf. It is applicable to all electronic communications regardless of the physical location (school, office, home, or any other offsite location) of the user.

Prohibited Use
The Bullock County School District' electronic communications programs shall not be used for the creation or distribution of any content that:

- Discloses unauthorized or restricted information to inside or outside parties via electronic communications, including restricted or confidential information that would violate the privacy of individuals or violate any other local, state, or federal laws including, but not limited to FERPA and HIPAA.
- Contains private information such as student grades, discipline incidents, suspensions, social security numbers, special education status, or Individualized Education Plans in cases where it would violate FERPA.
- Discloses personal information regarding students, faculty, staff, or parents to third parties.
- Contains information that pertains to someone other than the addressee (For instance, do not address E-mail~~s~~ to numerous individuals that contains private information that does not apply to all of the recipients).
- Defames, slanders, or libels another person or organization.
- Contains or links to pornography or other content inappropriate for K-12.
- Contains content that may be considered offensive or discriminatory, including, race, gender, hair color, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin.
- Contains content or files that violate any copyright or trademark law. Users should be aware that passing on E-mails that contain copyrighted or trademarked material may make them liable in copyright or trademark infringement cases even though they were not the original sender.
- Intentionally contains malicious or harmful software such as computer viruses and spyware.
- Contains fraudulent, harassing, or intimidating content.
- Violates any license governing use of software.

- Is intended for personal or private financial gain.

In addition, should employees receive electronic communications that contain such information, they should not forward such messages on to others whether inside or outside the System.

Personal Use
Except in cases of emergency, users should refrain from sending and reviewing personal E-mails during work hours. The content of personal E-mails, whether being received or sent, must also conform to the standards listed above as prohibited, and other restrictions that may be found in the Bullock County School District Employee Acceptable Use Policies. Users should immediately delete inappropriate E-mails and inform the sender about the restrictions on acceptable content.

Bullock County School District E-mail addresses shall not be used for non-work related shopping, subscriptions, memberships. In addition, Bullock County School District E-mail addresses should not be used on personal websites, blogs, social networking accounts, online forums, or any other electronic medium.

E-mail Filtering
Bullock County School District attempts to block offensive messages and spam from entering our System; however, this process is not 100% effective. Employees should report offensive and spam messages by forwarding them to the email listed in the spam summary or by contacting the Technology Department. Such messages should never be intentionally forwarded on to others whether inside or outside the Bullock County School District E-mail directory.

Mass E-mails
E-mails intended for all employees in the Bullock County School District System must be approved by the Superintendent, Director of Communication, his/her designee, or the District Technology Coordinator prior to be being sent.

Monitoring and Waiver of Privacy
Bullock County School District is not obligated to monitor E-mail messages; however, authorized administrators of the Bullock County School District may monitor messages without prior notice. Furthermore, electronic messages and files stored on Bullock County School District computers or stored elsewhere using a Bullock County School District E-mail or user account are deemed to be the property of Bullock County School District. Therefore, Bullock County School District employees and others to which this Acknowledgement applies shall have no expectation of privacy in anything they store, send, or receive on the System's electronic communications systems such as the E-mail system. Employees and others to which this Acknowledgement applies waive any right of privacy they might have in anything they create, store, or receive on the System's computers or electronic communications systems.

Reporting of Violations and Enforcement
Bullock County School District cannot guarantee that users will not occasionally receive offensive or inappropriate E-mails from outside the System or from fellow employees. Employees may report the matter to an immediate supervisor, the Communication Department, or the Technology Department should they feel an incident warrants further investigation.

Any employee found to have willfully misused any form of electronic communications as outlined in this Acknowledgement and in the Employee Handbook may be subject to disciplinary action. These actions may include the suspension or loss of E-mail, web, or other electronic communication privileges; or a verbal or written reprimand. A second violation of an employee may result in an adverse personnel action such as suspension or termination.

Disclaimers

In order to protect the System and the individual, all account holders shall use the disclaimer provided by the System on every E-mail sent. Individuals should be aware, however, that disclaimers do not offer any legal protection in the cases of defamation and libel. In addition, the presence of disclaimers may not entirely protect the sender from civil litigation or criminal prosecution.

Legal Actions

Should any legal actions, civil or criminal, take place which require the production of Bullock County School District' employees E-mails or electronic files, the System may comply with properly executed legal requests to the extent possible. All legal consequences and associated penalties for civil or criminal violations~~,~~ shall be the sole responsibility of the account holder and not that of the Bullock County School District, unless otherwise found by a court of law.

Indemnification

Employees and others to which the Acknowledgement applies agree to indemnify Bullock County School District for any losses, costs, or damages, including reasonable attorney fees, incurred by Bullock County School District relating to, or arising out of, their violation of this Acknowledgement.

Modifications

Bullock County School District may change the provisions of this Acknowledgement. Posting such modifications on the System's electronic communications system or sending such modifications by e-mail, fax, or U. S. Mail shall constitute proper notice of such modifications. However, no one, including principals or supervisors, may modify this policy in writing or verbally without the consent of the Superintendent.

Acknowledgement

I acknowledge that I have read and understand these risks and conditions, and in consideration of my use of the Bullock County Public School's computers and/or electronic communications systems. I agree to comply with the terms stated herein. I understand that I can seek further training or explanation regarding the content of this document by contacting my Principal, Supervisor, or the Technology Department.

Restrictions on Parents Posting Images of Students (who are not their own children) to Social Media (Not Implemented)

With respect to pictures of students being posted online on sites that are not on our servers, we are trying to prohibit this for our staff and discouraging it for parents. The number of complaints we have been getting because a parent will take pictures of children who are not theirs and post them online has risen sharply in the last two years. For this reason we have tried to support our schools in discouraging parents from posting pictures of other children on the web. Coming to school is different than joining a little league team or some other voluntary activity. I don't think the classroom teacher or the school could give an individual the right to post pictures of his/her class online without having control of the site and ensuring that every other parent has agreed to this and has access. From our department's standpoint, we think all material posted online about school should be on our servers or a server such as Edgenuity which we have control over and administrative access to.